



Delinea Platform

Administrator Guide

Version: 2024

Publication Date: 7/2/2025

Delinea Platform Administrator Guide

Version: 2024, Publication Date: 7/2/2025

© Delinea, 2025

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Administrator Guide	1
Introducing the Delinea Platform	34
Benefits	34
Secret Server	34
Robust Identity and Federation Services	34
Privileged Remote Access (formerly RAS)	34
Privilege Control for Servers	35
Identity Threat Protection	35
Privilege Control for Cloud Entitlements	35
Integrations and Marketplace	35
NextGen Mobile Application	35
Near-Perfect Uptime	36
Uptime: Delinea Platform vs. Legacy SaaS	36
Quick Start Guide	36
Provision and Log In to the Platform	37
Enable Domain Users to Log into the Platform	38
Install the Delinea Connector and Authorize AD Accounts	38
Assign Your Business Domain User to the System Administrator Group	38
Synchronize the System Administrator Group to Secret Server	39
Access Secrets as a System Administrator	39
Add Federated User Accounts	39
About Local User Accounts	40
Assign Roles and Permissions to Users and Groups	40
Set Up and Use Privileged Remote Access	40
Launch a PRA Session	41
Set Up Continuous Identity Discovery	41
About Multi-factor Authentication	41
Delinea Platform Interface	42
Primary Left Navigation Menu	42
Secondary Navigation	43
Hover over a menu item	43
Click a menu item	44
Global Search	46
Favorites and Recents	47
Favorites	47
Recents	48
Filtering in List Pages	48
Using Quick Filters	49
Using the Query Builder	49
Release Notes	50
Please Wait...	51
Spring (Q2) 2025 Release	51

Table of Contents

Secret Server on Platform	51
Continuous Identity Discovery (CID)	51
Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)	51
Analytics	52
Identity Lifecycle Management (ILM)	52
Privileged Remote Access (PRA)	52
Connection Manager (CM)	52
Inventory	53
Identity and Federation	53
Engine Management	53
Marketplace and Integrations	53
Other Updates	54
Winter (Q1) 2025 Release	54
Secret Server (SS) on Platform	54
Continuous Identity Discovery (CID)	55
Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)	55
Analytics	55
Privileged Remote Access (PRA)	56
Connection Manager (CM)	56
Privilege Control for Servers (PCS)	56
Inventory	57
Identity & Federation	57
Engine Management	57
Marketplace & Integrations	58
Other Updates	58
Fall (Q4) 2024 Release	58
Secret Server (SS) on Platform	58
Continuous Identity Discovery (CID)	59
Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)	59
Privileged Remote Access (PRA)	59
Connection Manager (CM)	59
Privilege Control for Servers (PCS)	60
Identity and Federation	60
Platform Engine Management	61
Integrations and Marketplace	61
New Authenticator Mobile App	61
Other updates	61
Summer (Q3) 2024 Release	62
Secret Server on Platform	62
Remote Access Service (RAS)	63
Connection Manager (CM)	63
Identity & Federation	63
Audit	64
Permissions	64

Table of Contents

Engine Management	64
Marketplace & Integrations	64
New Authenticator mobile app	65
Other updates	65
Spring (Q2) 2024 Release	65
Secret Server on Platform	65
Privileged Remote Access (PRA)	65
Connection Manager (CM)	66
Inventory	66
Audit	66
Marketplace & Integrations	67
Identity & Federation	67
Platform Engine Management	67
Privilege Control for Servers	67
Delinea Mobile App	68
Web Password Filler (WPF)	68
Other updates	68
Winter (Q1) 2024 Release	69
Secret Server on Platform	69
Privileged Remote Access (PRA)	69
Connection Manager (CM)	69
Audit	69
Marketplace & Integrations	69
Identity & Federation	69
Other updates	70
Fall (Q4) 2023 Release	70
Secret Server on Platform	70
Privileged Remote Access (PRA)	70
Web Password Filler (WPF)	70
Connection Manager (CM)	70
Integrations and Marketplace	70
Identity & Federation	71
Other updates	71
Summer (Q3) 2023 Release	72
Secret Server on Platform	72
Privileged Remote Access (PRA)	72
Web Password Filler (WPF)	72
Connection Manager (CM)	72
Audit	72
Marketplace & Integrations	72
Identity & Federation	73
Other updates	73
Spring (Q2) 2023 Release	74
New Hosting Regions	74

Table of Contents

Behavioral Analytics (Private Preview)	74
Permissions Service	74
Improved Home Screen	74
Marketplace	74
Tenant Customization	75
Winter (Q1) 2023 Release	75
Seamless Integration with Secret Server Cloud	75
Next-Gen Privileged Remote Access	75
Robust Identity and Federation Services	75
Marketplace	75
Foundational Shared Services	75
Preview Program	76
Public Preview	76
Opt In	76
Opt Out	76
Current Public Preview Features	76
Private Preview	77
Current Private Preview Features	78
Platform Architecture	79
Customer Firewall Requirements	79
Determining Your Tenant's Customer Service Bus and Engine Response Bus	79
U.S. Tenants	79
Non-US Tenants	80
Inbound Filtering	82
Ports and Network Communication	83
Privileged Remote Access	84
Delinea Connector	84
Privilege Control for Servers (PCS) Agent	85
Notification Services	85
Tenant IP Restrictions	86
Key Benefits	86
Submitting an IP Restriction Request for the Platform	86
Delinea Expert	86
Accessing Delinea Expert	87
Interaction Tips	87
Additional Uses	88
Troubleshooting Delinea Expert	88
Known Issues	89
Information Sources	89
Access to Delinea Expert	89
Privacy & AI Transparency	90
AI Transparency Notice - Delinea Expert	90
Where are the Question Prompts and Responses Stored?	90
Are Question Prompts Sent or Routed to "Open" or "Public" AI Models?	90

Table of Contents

Does Delinea use Prompts for Fine-tuning or to Improve the Overall Responses?	90
Do Delinea Employees Have Access to the Prompts or Responses?	90
Is Use of Delinea Expert Required?	90
How were the AI-generated Search Results Tested?	91
Does Delinea Expert Process Personal Data?	91
Vaulting Secrets on the Platform	91
For New Business Users	91
For New Administrators	91
For Existing Secret Server Customers	91
Accessing Secret Server from the Platform	91
Secrets	92
Creating Secrets	92
Checking Out Secrets	92
Launching Secrets	93
Secret Folders	93
Creating Folders	93
Moving Secrets Between Folders	93
Credential Management	93
Discovery	93
Distributed Engines	94
Remote Password Changing	94
Auditing Privileged Account Activity	94
Advanced Session Recording and Management	94
Audit Logs	95
Alerts	95
Built-in Reports	95
QuantumLock	95
Inventory	96
Managing Computer Assets	96
Inventory Permissions	97
Viewing Your Computers Inventory	97
Searching Your Inventory	97
Using Search and Filters	97
Using Query Builder	98
Drilling into Details	98
Logging In to a Computer	99
Disabling Active Inventory	99
PCS Policies	99
Grouping with Computer Collections	99
Creating a New Computer Collection	100
Modifying a Computer Collection	100
Deleting a Computer Collection	100
Assigning User Permissions on Computer Collections	101

Table of Contents

Interaction Between Collection-Based and Role-Based Permissions	101
Common Access Control Configurations	102
Permissions Reference	102
ITP/PCCE Inventory	103
Inventory Types	104
Inventories User Interface	104
Searching by Custom Properties	105
Sorting the Inventory Table	105
Using Other Views	105
Configuring Table Columns	106
Exporting a Table as CSV	106
Using Tags	107
Filtering an Inventory Table	107
Inventory Filter Properties	107
Identities	108
Groups	111
Assets	112
Memberships	113
Access Policies	114
Privileges	116
Activities	116
Insights	118
AI-Driven Auditing (AIDA)	118
Data Privacy and Processing	118
Session Recording	119
Reviewing Session Recordings	119
Enabling Session Review	119
Launching a PRA Session with Session Review Enabled	119
Enabling Metadata Recording	120
Viewing Sessions	121
Viewing Session Recordings	124
Video Controls	125
Analyzing a Recording with AIDA	126
Performing an Analysis	126
Viewing Recording Details	127
Viewing the Heatmap	129
Commenting and Flagging a Session	129
Sharing Sessions	130
Reviewing Audit Logs	130
Accessing Audit Logs	130
Viewing The Audit Log	131
Customizing the Audit Log Table	131
Filtering Events	132
Selecting Audit Levels for Display	132

Table of Contents

Downloading Event Log Data	133
Audit Collector Services	134
Engine Management Services	148
Identity Services	148
Identity Federation Services	150
MFA Providers Services	151
Permissions Services	152
Policy Services	152
Privileged Remote Access Services	153
Registration Services	154
Secret Server Services	154
Session Recording Services	161
Tenant Profile Services	161
Analytics	161
Permissions	161
Identifying Alerts	161
Analytics Dashboard	162
Interpreting Dashboard Analytics	162
Current Risk Score	162
Riskiest Accounts	162
Latest Alerts	162
Alerts Over Time	162
Activity	162
Analytics Findings and Risk	163
Risk Scores	163
Types of Alerts	163
Discovery	165
Combined Discovery	165
Users and Groups	169
External User Accounts vs. Local User Accounts	170
Avoid Adding Local User Accounts	170
Adding Users	171
Adding Local Users	171
Add Local Users	171
Bulk Importing Local Users	173
Service Users	176
Add Service Users	177
Managing User Accounts	179
View User Accounts	179
Overview Tab	181
Status	182
Account	183
Advanced Settings	184

Table of Contents

Secret Server Details	185
Groups Tab	186
Roles Tab	187
MFA Redirection Tab	187
Typical MFA Redirection Use Cases	188
Configure MFA Redirection	188
Additional Attributes Tab	188
Activity Tab	189
Policy Summary Tab	190
Secret Server Settings Tab	192
Managing Your User Profile	192
Account	193
Preferences	194
Launcher Settings	195
Security tab	195
Passcodes	195
Secret key, Key algorithm, OTP digits, and Period	196
Applications	196
Activity	196
Roles	197
Managing Groups	197
Predefined Groups	197
Types of Groups	198
Adding a Group	198
Adding Users to a Group	199
User Directory Service Configuration	200
Additional Attributes	201
External Directory Group Allowlist	202
Create or Update an External Group List	203
Delete Groups from the External Group List	203
Roles and Permissions	203
Unified Roles and Permissions in Secret Server and Platform	203
Built-in Roles	204
Custom Roles	204
Permissions	204
Users, Groups, Roles, and Permissions	204
Edit Role Permissions	204
Edit Role Members (Groups)	207
Delete a Role	208
Assign a Group to a Role	209
Create a New Role	210
Add Members (Groups) to a Role	211
Platform Permissions	212
Miscellaneous Permissions	212

Table of Contents

Administration Permissions	215
Behavioral Analytics Permissions	217
Platform Audit Permissions	218
Delinea Expert Permissions	219
Posture Check Permissions	219
Identity Permissions	219
Inventories Permissions	219
Analytics Management Permissions	220
Marketplace Permissions	220
Remote Access Permissions	220
Vaultbroker Configuration Permissions	221
Secret Server Permissions	221
Platform Engine Management	233
Engine Management Components	233
Engine Management Architecture	235
Server Hardware and System Requirements	235
Engine Security	237
Engine Status	237
Account Permissions and Roles	238
Network Communication	239
Protocols	240
HTTP Proxy Setup	240
Specifying HTTP Proxy Settings Using bitsadmin	241
Specifying HTTP Proxy Settings Using the Registry	242
About Delinea Platform Engine Sites	242
About the Delinea Platform Engine	243
Managing Engine Sites	243
Engine Site Preview Panel	243
Creating a Site	244
Editing a Site	244
Deleting a Site	245
Managing Platform Engines	246
Adding a Platform Engine	246
Copying a Platform Engine	248
Adding Capabilities to a Platform Engine	249
Automatic Platform Engine Update	250
Manual Platform Engine Update	251
Uninstalling an Engine from the Platform	251
Manually Uninstall an Engine from Host Machine	252
Windows Platform Engine and Log Directories	252
Linux Platform Engine and Log Directories	253
Platform Engine Log Levels	253
Adjusting Windows Platform Engine Log Levels	253
Adjusting Linux Platform Engine Log Levels	254

Table of Contents

Checking Logs in the Engine Management Interface	254
Understanding Engine Workloads	255
Workload Deployment States	256
Workload Log Directories	256
Monitoring Workloads	256
Restarting Workloads	257
Audit Collector Workload	257
Editing Audit Collector Settings	257
Audit Collector Account Permissions	258
Command Relay Workload	259
Command Relay Prerequisites	260
Editing Command Relay Settings	260
Command Relay Account Permissions	261
The DelineaZone	262
Switching Command Relay Service Accounts	263
PRA Workload	263
Sizing for the PRA Workload	264
Troubleshooting the PRA Workload	265
ITP for Active Directory Workload	266
Prerequisites	266
Adding ITP for Active Directory	266
Editing ITP for Active Directory	266
AD Rapid Discovery Workload	267
Deployment	267
Editing AD Rapid Discovery Settings	268
Setting AD Rapid Discovery Account Permissions	268
Troubleshooting Platform Engine	269
Engine Doesn't Appear, is Outdated, or Status Shows "Failed"	269
Engine Upgrade Problems	269
Need to Manually Reinstall Engine	269
Workload Status Shows "Failed"	270
Getting 400s When Engine is Trying to Register	270
Engine and Logs Directory Structure	270
Active Directory Connector	271
Determining Whether You Need the Delinea Connector	272
Installing the Delinea Connector	272
Server Requirements	272
Account Permission Requirements	273
Platform Permissions	273
Delinea Connector Permissions	273
Connector Security Permissions	273
Alternate Accounts and Organizational Units Permissions	273
Setting Read Access Permission to the User Account Container or Organizational Unit	274
Setting Read Access Permission to User Account Container with Powershell	274

Table of Contents

Downloading the Delinea Connector and Getting a Registration Code	275
Installing and Configuring the Delinea Connector	276
Enabling Auto-Update for the Delinea Connector	279
Updating the Delinea Connector	280
Checking the Delinea Connector Status	281
Supported AD Group Types on the Delinea Platform	282
Why Distribution Lists Are Not Supported	282
Using Connector Best Practices	283
Supporting User Authentication for Multiple Domains	283
Configuring Authentication for Trusted Domains	283
Configuring Authentication for Multiple Forests without Trust	285
Delinea Connector Redundancy	286
Installing Additional Delinea Connectors	286
Additional Information	286
Troubleshooting the Delinea Connector	287
Platform Can't Map a Federated User to an AD User	287
Can't Add Local User with Duplicate Login ID	287
Invalid Certificate Error Installing Connector	287
Missing or Unverified Certificate Error Installing Connector	287
Unhandled Exception Error Installing Connector	288
Certificate Check Error Registering Connector	288
Failed to Connect Error Registering Connector	289
Delinea Connector Configuration Application Stalls	289
Connector Fails to Connect to Platform	289
Delinea Connector Auto-update not Working	289
Authentication Fails After Connector Installed and Active	289
Where Can I Access the Delinea Connector Logs?	290
What are the Default Rotation Settings for Connector Logs?	290
What are Best Practices for using Federation and Active Directory Together?	290
Can't Query Active Directory Users or Groups After Connector Installed and Active	290
Privileged Remote Access	290
Setting Up the PRA Engine	291
PRA Requirements	291
Useful Tools	292
Sizing for PRA Engine Linux Hosts	292
Setting Up a PRA Engines Site	293
Naming a PRA Site	294
Renaming PRA Site	295
Configuring PRA	297
Customize the Keyboard Layout	297
Font Smoothing	298
Kerberos Authentication	298
Installing PRA Engines	301
Engine Rules	301

Table of Contents

Installing the Remote Access Engine	301
Installation Script Rules	303
Run the Installation Script	303
Configuring the PRA Engine to Use a Proxy Server (Optional)	303
Activating PRA Engines	305
Adding Secret Templates to PRA	306
Secret Server Cloud	306
Secret Server On Premises	306
Uninstalling PRA Engines	307
Automated Uninstallation	308
Manual Uninstallation	309
Upgrading Standalone PRA Engine to the Delinea Platform Engine	309
Prerequisites	309
Recommended Best Practices	310
Automatically Upgrading PRA Engines to the Delinea Platform Engine	310
Manually Upgrading a Standalone PRA Engine to the platform Engine	313
Upgrading the Standalone PRA Engine While Working in an Active Session	315
Using the PRA Engine	316
PRA and the Delinea Platform	316
PRA Sites	316
Naming a PRA Site	316
Launch a PRA Session	317
From Secret Server On-Premises	319
Update PRA Engines	319
Updating a PRA Engine	320
Manually Updating a PRA Engine	322
Accessing Remote Applications With PRA	322
Prerequisites	322
Launch a Remote Application	322
Add a New Remote Application	326
Edit a Remote Application	327
Using the Delinea Menu	328
Transfer Files	330
Session Information	330
Settings	330
Screenshot	331
Clipboard	331
Enter Full Screen	333
Disconnect	333
Transferring Files With PRA	334
Prerequisites	334
Download a File	335
Upload Files	338
Queue Tab	339

Table of Contents

Current Limitations	342
Accessing Private Web Applications With PRA	343
Prerequisites	343
Creating a New Web Application	343
Launching a Web Application	344
Public to Private URL Mapping	346
Understanding PRA Permissions and Roles	346
Permissions Applicable Only for Secret Server On-Premises	349
RemoteApp Permissions	349
Web Application Permissions	350
Permissions From Other Delinea Platform Services	350
Hardening the PRA Engine Host	351
General Hardening Steps	351
Restrict Incoming Port Access to All PRA Engine Servers	351
Remove Unnecessary User Groups	351
Rename Default Accounts	352
Disable Services	352
Restrict Network Protocols	352
SSL/TLS Settings	352
System Admin - Universal	352
Network SSH/OpenSSL:	352
Auditing	353
CIS standards	354
Ubuntu	355
System Ubuntu:	355
Directories, Files and Permissions	356
Red Hat Enterprise Linux - RHEL	356
System RHEL:	356
Directories, Files and Permissions:	357
Network SSH/OpenSSL:	357
Understanding PRA Entitlements	357
Understanding PRA Workloads on the Delinea Platform Engine	358
PRA Troubleshooting	358
Failed to Connect to the Target Machine	358
RDP Supported Authentication Methods	358
The Engine is Configured Properly But a Connection to the Target Cannot Be Established	359
Accessing Logs on the Engine Server	359
Unable to Launch SSH Sessions via Secret Server Distributed Engine	360
Issues Connecting to On-Prem Secret Server	361
Troubleshooting Connection Issues Between Secret Server On-Premises and the Delinea Platform	361
The Engine Shows as "Offline"	362
Unable to Open an SSH Session From the Web UI	363
Unable to Open an RDP Session From the Web UI	363
Engine Seems to be Functioning in an Unexpected Manner	363

Table of Contents

Setting a Static UUID	364
Issues Installing the PRA Engine	366
Warnings That Can Occur During Installation	367
Errors That Can Occur During Installation:	367
Uninstallation of the PRA Engine is Not Working From the Web UI.	368
Using Start/Stop Commands	369
SAML and OIDC Federation	369
Platform Federation Integrations	370
Supported SSO Approaches	370
SP-Initiated SSO	371
IDP-Initiated SSO	372
Managing Federations	373
Add a Federation Service Provider	373
Enable a Federation Service Provider	373
Delete a Federation Service Provider	374
Advanced Settings (SAML only)	374
Advanced Settings (OIDC only)	374
Re-authentication with the IdP	375
Prompt for Re-authentication (OIDC only)	375
Attribute Mappings	376
Mapping Federated Groups	377
Introduction to Group Mapping	377
Configuring Group Mapping	378
Mapping Federated Users	380
Map a federated user to an existing directory user	380
Debugging	381
Analyzing Captured Logs	382
Integrating AD FS	383
Prerequisites	383
Setting Up AD FS with SAML	384
Retrieve AD FS metadata	384
Add the Provider to the platform	384
Initial AD FS Setup	385
Configure assertion attributes	387
Attribute Mappings	388
Add the Provider to the Platform	388
Settings	388
Advanced Settings	389
Attribute Mappings	389
Group Mappings	389
User Mappings	390
Domains	390
Integrating Auth0	390
Prerequisites	390

Table of Contents

Build an Auth0 SAML Application	390
Add the Provider to the Platform	392
Settings	393
Advanced Settings	393
Attribute Mappings	393
Adding Custom Claims	394
Group Mappings	394
User Mappings	394
Domains	394
Build an Auth0 OIDC Application	394
Add the Provider to the Platform	396
Settings	396
Attribute Mappings	396
Group Mappings	396
User Mappings	396
Domains	396
Integrating BlokSec	396
Integrating Celestix	397
Integrating Entra ID	397
Prerequisites	397
Build an Entra SAML Application	397
Attributes and Claims Mappings	401
Domains	402
Add the SAML Provider to the Platform	404
Settings	404
Advanced Settings	405
Attribute Mappings	405
Group Mappings	405
User Mappings	406
Domains	406
Build an Entra OIDC Application	406
Add the OIDC Provider to the Platform	409
Settings	410
Attribute Mappings	411
Group Mappings	412
User Mappings	412
Domains	413
Add the Platform	413
From Your Entra Application	413
From the Platform	415
Integrating Entrust	415
Prerequisites	415
Build an Entrust SAML Application	416
Add the Provider to the Platform	419

Table of Contents

Settings	420
Advanced Settings	420
Attribute Mappings	421
Group Mappings	421
User Mappings	421
Domains	421
Build an Entrust OIDC Application	421
Add the Provider to the Platform	426
Settings	427
Attribute Mappings	427
Group Mappings	427
User Mappings	427
Domains	428
Test Configuration	428
Known limitation(s)	428
Integrating Google	428
Prerequisites	428
Build a custom Google Workspace SAML app.	429
Add the Provider to the Platform	429
Settings	429
Advanced Settings	430
Attribute Mappings	430
Group Mappings	431
User Mappings	431
Domains	431
Update Google Workspace	432
Turn on Your SAML App	433
Test Your SAML App	433
Build a Custom Google OIDC App	434
Add the Provider to the Platform	436
Settings	436
Attribute Mappings	436
Group Mappings	436
User Mappings	437
Integrating Okta	437
Prerequisites	437
Build an Okta SAML Application	437
Add the Provider to the Platform	442
Settings	442
Advanced Settings	443
Attribute Mappings	443
Group Mappings	443
User Mappings	444
Domains	444

Table of Contents

Build an Okta OIDC Application	444
Add the Provider to the Platform	445
Settings	446
Attribute Mappings	446
Group Mappings	446
User Mappings	447
Domains	447
Integrating OneLogin	447
Prerequisites	447
Build a OneLogin SAML Application	447
Add the Provider to the Platform	451
Settings	451
Advanced Settings	452
Attribute Mappings	452
Group Mappings	452
User Mappings	452
Domains	452
Build a Onelogin OIDC Application	453
Add the Provider to the Platform	456
Settings	456
Attribute Mappings	456
Group Mappings	456
User Mappings	456
Domains	456
Test Configuration	457
Known limitations	457
Integrating Ping Identity	457
Prerequisites	457
Build a Ping Identity SAML Application	457
Add the Provider to the Platform	459
Settings	459
Advanced Settings	460
Attribute Mappings	460
Group Mappings	460
User Mappings	460
Domains	461
Post-configuration to Ping Identity Application	461
Update Entity ID	461
Attribute Mappings	461
Activate the Application	461
Map Ping Identity and Platform Groups	462
From Your Ping Identity Application	462
From the Platform	463
Test Connection	463

Table of Contents

Troubleshooting	464
Build a Ping Identity OIDC Application	466
Configure the Application on Ping Identity	467
Add the Provider to the Platform	467
Settings	467
Attribute Mappings	468
Group Mappings	468
User Mappings	468
Domains	468
Post-configuration to Ping Identity	469
Update Redirect URIs	469
Attribute Mappings	469
Enabling the Application	470
Test Connection	470
Integrating RSA SecurID	471
Troubleshooting Federated Group Mapping	471
Platform Group Sync Overwrites Secret Server Groups Every Four Hours	471
Multi-Factor Authentication	472
About MFA	473
Creating Authentication Profiles	473
View Authentication Profiles	474
Add a New Authentication Profile	474
Authentication Challenges	476
Assigning a Login Authentication Profile	476
Global Security Settings	478
Security Questions	478
Security Devices	479
Creating Identity Policies	480
Create and Assign an Identity Policy	480
Create a Conditional Access Policy	481
Update an Identity Policy	484
Authentication	485
Services	486
Authentication Rules	486
Browser Session Parameters	488
Delinea Mobile Application Session Parameters	488
Other Settings	488
User Security	490
Self Service	490
Password Settings	492
OATH OTP	495
RADIUS	495
User Account Settings	496
Authentication Settings	496

Table of Contents

Summary	501
Using a FIDO2 Security Key	501
Using MFA for Secrets	501
Availability	501
Default MFA Profile	501
Assigning MFA to Secrets	502
Assign MFA to an Individual Secret	502
Assign MFA to a Secret Policy	502
Assign MFA to Secrets Through a Bulk Operation	502
Applying an MFA Profile to All Enabled Secrets	503
Considerations for Assigning MFA to Secrets	504
Configuring Corporate IP Ranges	504
Add an IP Range	505
Edit an IP Range	505
Delete an IP Range	505
Configuring IWA	505
Prerequisites	506
Enabling IWA Service on the Delinea Connector	506
Obtaining a Delinea Connector IWA Host Certificate	507
Using an Automatically Generated Delinea Connector IWA Host Certificate	507
Importing a Certificate	508
Generating a Self-Signed Delinea Connector IWA Host Certificate	509
Downloading the Delinea Connector IWA Host Certificate	510
Distributing the Delinea Connector IWA Host Certificate for Agent Installation	510
Verifying IWA Over HTTPS	514
Allowing IWA Connections for Users in the Default Policy	515
Using IWA With Identity Cookie	515
Using IWA to Authenticate Application Access	516
Disabling IWA	516
Configuring OTP Client Authentication	516
Create a Group for OTP Users	517
Define an Identity Policy for OTP Authentication	517
Create and Onboard an OTP User	518
Platform Login Flow	519
Summary	519
Contractor and Vendor Access	519
Prerequisites	520
Local Users	520
Bulk Import of Vendors	520
Active Directory	520
Federated Vendors	521
Managing Vendor Entitlements with Active Directory	521
Managing Vendor Entitlements with Federation	524
Requirements	524

Table of Contents

Adding a New Claim to EntraID App Registration	524
Configuring Attribute Mappings in Delinea Platform	527
MFA Providers	528
Configuring Duo Authentication	528
Prerequisites	528
Build a Duo Application	528
Add Duo to the Platform	530
Enrolling Duo Users	531
Duo Policies	532
Configuring RADIUS Authentication	532
Radius Authentication Overview	532
Configuring a RADIUS Server	532
Configuring the Delinea Connector as a RADIUS Client	534
Using RADIUS Authentication	536
Registered Apps	537
Entra ID API Integration	537
Prerequisites	538
Create a Delinea-Managed Registered App	538
Add a Delinea-Managed Registered App	538
Grant Delinea Permission to Create and Manage App Registrations in Azure	539
Create a Customer-Managed Registered App	540
Create an Azure Application Registration	541
Create a Customer-Managed Registered App on the Delinea Platform	545
Update the Azure App Registration with the Platform Callback URL	548
Automating Entra ID Integration Setup	549
Test the API-Based Entra ID Integration	549
Entra ID FAQs	550
Can I use the Connector with the Entra ID API integration simultaneously?	550
Can I use Entra ID Federation and Entra ID API integration simultaneously?	550
How is adding Entra ID users different from adding federated users?	550
How is Entra ID Federation user mapping different from standard federation?	550
What if users can't log in after the integration is set up?	550
What happens if I disable a registered app?	550
Can I Create a Registered App for Each API Permission?	550
What validations and errors might arise when creating a registered app?	551
What customer-managed registered app configurations create different outcomes?	551
What is the scope of the API permission "Entra ID - Read"?	551
Will we eventually have the same browsing experience for AD and Entra ID?	551
How long does the Platform take to detect and reflect changes from Entra ID?	552
How do user attributes (e.g. mobile number) propagate from Entra ID to Platform?	552
What are the advantages of configuring the Entra ID integration using the Delinea-managed registered app?	552
Where is the registered app I created as part of the private preview?	552
How are secrets managed using the Delinea-managed app?	552

Table of Contents

How can I resolve Delinea-managed app consent errors?	552
Can I delete a Delinea-managed app?	552
Webhooks	552
Managing Webhooks	553
Prerequisites	553
Creating a Webhook	553
Managing Webhooks	555
Webhook Logs	557
Verifying a Webhook	559
Calculating Hash	560
Integrating Microsoft Sentinel	561
Prerequisites	561
Configuring Microsoft Sentinel	562
Creating a Logic App in Sentinel	562
Setting up Sentinel Log Analytics	563
Integrating Webhooks and Microsoft Sentinel	567
Verifying Logs for the Microsoft Sentinel Webhook	568
Integrating Splunk Enterprise	570
Prerequisites	570
Setting Up Splunk Enterprise	570
Creating a Certificate in Zero SSL	570
Configuring a Certificate in OpenSSL	572
Integrating Webhooks and Splunk Enterprise	574
Configuring Splunk Enterprise HTTP Event Collector	574
Creating Webhooks for Splunk Enterprise	579
Verifying Logs for Splunk Webhook	581
Integrating Splunk Cloud	582
Prerequisites	582
Configuring Splunk Cloud	582
Creating an HTTP Event Collector in Splunk Cloud	583
Configuring Webhooks on the Delinea Platform	584
Creating a Webhook	584
Testing Webhooks on the Delinea Platform	586
Verifying Splunk Cloud Integration with the Delinea Platform	586
Verifying Integration in Splunk Cloud	586
Verifying Integration on the Delinea Platform	586
Integrations and Marketplace	587
Integrations	587
Sorting	587
Filtering Options	588
Integration Details	589
Applications	590
Application Details	591

Table of Contents

Quick Filters	593
Download Center	594
Mobile Access	598
Administrators	598
Users	598
Platform Notifications	599
Authenticating with Platform APIs	599
Privilege Control for Servers	600
The Privilege Control Agent	600
PCS Policies	600
Inventory	600
Engine Management	600
Audit Collector	600
Command Relay	601
Next Steps	601
Setting Up PCS	601
Prerequisites to PCS Installation	601
PCS Installation Overview	601
Step 1: Configure Firewall Ports for PCS	602
Step 2: Set Up PCS Service Accounts	602
Step 3: Install the Delinea Connector on Managed Servers	602
Step 4: Enable IWA Service on Connectors	602
Step 5: Install the Delinea Platform Engine on Managed Servers	602
Updating the Platform Engine Management Settings	603
Updating the Platform Engine	603
Step 6: Install the Delinea Agent on Managed Servers	604
Requirements for Delinea Agent Installation	604
Checking for Agent Installation	605
Downloading the Agent	605
Installing the Linux Agent	605
Installing the Windows Agent	606
Step 7: Scan Computer Inventory	608
Step 8: Set Up Authentication Profiles for PCS	608
Step 9: Set Up PCS Policies	608
Step 10: Set Up Audit and Session Recording	608
Viewing Audit Session Recordings	609
Step 11: Set Up Use My Account	610
Supported Operating Systems for Agents	610
Supported UNIX/Linux Platforms	610
Supported Windows Platforms	612
Setting Up PCS Policies	612
Viewing Policies	612
Deployment Status	613

Table of Contents

Creating a Policy	613
Policy Details	614
Command Groups	614
Creating Commands	614
Creating Command Groups	616
Adding Command Groups to the Policy	616
Modifying Commands and Command Groups	616
Policy Subjects	617
Policy Targets	617
Policy Conditions	618
Policy Controls	618
Enabling IWA on the Default Identity Policy	619
Setting Up Use My Account	621
Using Delinea OpenSSH	621
Using OS Stock Version of OpenSSH	621
Using Automatic Script for UMA	621
Using Manual Steps	622
Test Use My Account	623
Setting Up a Certificate for Internal MS CA	624
Joining Linux/UNIX Hosts to a Domain/Zone	636
Using Adjoin on New Computers	636
Running Adjoin Requires UNIX and Active Directory Privileges	637
Specifying the Required Options	637
Pre-staging Before Using Adjoin on a New Machine	637
Log On to Verify Authentication After Joining the Domain	639
Using GPO on Platform	639
Using Commands	639
Controlling Access to Commands	639
What Command Rights Provide	640
Granting Access Using Command Rights	640
Examples of Windows Elevated Privilege Commands and Apps	640
Examples of Linux Elevated Privilege Commands and Apps	641
Linux PCS Template Commands	641
About Linux Match Paths	643
About Glob Expressions	644
Managing Agents	645
Installing Agents on Computers to be Managed	645
System Requirements	645
About the Deployment Process	645
Selecting a Target Set of Computers	645
Options for Deploying Privilege Control Agent Packages	646
Installing Silently Using a Configuration File	647
About the Sample Configuration Files	647
Setting the Parameters in a Custom Configuration File for the Installation Script	647

Table of Contents

Customizing the Return Codes for the Installation Script	652
Using Other Automated Software Distribution Utilities	653
About the Files and Directories Installed on the Agent	653
Joining an Active Directory Domain at a Later Time	653
Upgrading the Linux Agent	654
Uninstalling a Linux Agent	654
AD Orphan Object Cleanup Script	655
Installing the PowerShell Access Module	655
Creating and Using a Connection	656
Confirming Licenses	656
Running the Script	656
Using the Default Windows PowerShell Console	657
Enabling Logging	657
Troubleshooting PCS	657
Can't Find Log Files	658
Connection and MFA Issues	658
Can't Connect to Delinea Platform	658
Windows Diagnostics Error for MFA	659
MFA Zero Pass-Through Not Working	660
DirectControl Authentication Not Working on *nix	660
Policies	660
Can't Find User for Subjects	660
Policy Endlessly Activating or Deactivating	660
Active Policy Not Enforced	661
Inactive Policy Still Seems Active	661
Machine Not In Target List	661
Command Relay / Delinea Platform Engine	662
Increasing the Log File Detail Level	662
Frequently Asked Questions	662
Command Relay Secret Stops Working	663
Command Relay Can't Log In	663
IWA Doesn't Work When Installing Connector	664
Secret Server	664
Distributed Engine Not Working	664
Privilege Control for Servers Agent	665
Increasing the Log File Detail Level	665
Turning On Debugging for SSHD	665
Collecting Debugging Information	665
Frequently Asked Questions	665
Session Recording Stops Linux Agent Login	666
AD User Can't Log In on Linux	666
AD User Can't Run dzdo on Linux	667
Useful Commands and Tips for AD Client on *.nix	668

ITP and PCCE	677
Identity Threat Protection	678
Privilege Control for Cloud Entitlements	678
Setting Up ITP and PCCE	678
ITP/PCCE Inventory	679
Inventory Types	680
Inventories User Interface	680
Searching by Custom Properties	681
Sorting the Inventory Table	681
Using Other Views	681
Configuring Table Columns	682
Exporting a Table as CSV	682
Using Tags	683
Filtering an Inventory Table	683
Inventory Filter Properties	683
Identities	684
Groups	687
Assets	688
Memberships	689
Access Policies	690
Privileges	692
Activities	692
Identities	694
Filtering and Modifying the Identities Table	695
Insight into Identities Table Data	695
Using Filter Options	695
Customizing Identity Merging Rules	696
Account MFA Factors	698
Groups	699
Filtering and Modifying Groups Table	699
Insight into Groups Table Data	699
Assigning Alternative Group Names	700
Assets	700
Insight into Assets Table Data	700
Memberships	701
Filtering and Modifying Memberships Table	701
Using Filter Options with Memberships	701
Access Policies	701
Filtering and Modifying Access Policies Table	702
Privileges	702
Filtering and Modifying Privileges Table	702
Using Filter Options with Privileges	703
Activities	703
Filtering and Modifying Activities Table	703

Table of Contents

Collections	704
ITP-PCCE Collections vs. Computer Collections	704
System Collections	704
Custom Collections	708
Access Explorer	709
Direct vs. Indirect Access	709
Recurring Reports	713
Identity Posture	713
Using Apps Overview	714
Using Checks	715
Onboarding Process	715
Viewing the Checks Page	715
Best Practices for Checks	716
Diagnosing Issues with the Checks Side Panel	716
Admin and Privileged Access	720
Admin Access	720
Privileged Access	721
Shadow Admins	721
AWS Actions	721
Azure Permissions	723
Threat Center	724
Using Cases	724
Case Management	724
Automated Response Options	726
How to Review Cases	727
Viewing Alerts	730
Customizing the Display	730
Viewing Alert Details	731
Alert Properties	732
General Tab	732
Entities Tab	732
Evidence Tab	732
Resolving Alerts	734
Protect AI & LLMs within Cloud Apps	735
Visibility into AI Models Deployed in CSPs	735
Visibility into AI agents and services managed in CSPs	735
Visibility into AI Models Hosted on Cloud Assets	735
Access Control and Risk Mapping	735
AI Reports for Governance	736
Security Checks and Risk Assessments	736
Configuring Risk	736
Risk Types	736
Configuring Risk	737

Continuous Identity Discovery	738
Introduction	738
Overview	738
Step 1: Add CID Sources	738
Step 2: Review Checks for Non-Vaulted Entities	738
Step 3: Establish a Baseline	739
Step 4: Customize Privileged User Definitions	739
Step 5: Use Inventory for Advanced Filtering and Reporting	739
Next Steps	739
Discover Unvaulted Privileged Cloud Service Users	739
Discover PAM Bypassing	740
Discover Delegated Permissions	742
CID Manual and Bulk Vaulting	742
Create a CID Report	743
Setting Up CID Integrations	743
Identity Governance Administration	744
Current Capabilities	744
Identity Lifecycle Management	745
ILM Advantages for Users and Organizations	745
Stages: Joiner Mover Leaver (JLM)	745
Joiner	745
Mover	745
Leaver	746
ILM Setup and Configuration	746
User Types	747
About User Types	749
Governance System Settings	751
Sensitive Data Encryption (Key Manager)	751
Delivery System Time	752
Identity Management Settings	752
Data Generation Rules	753
Creating a Data Generation Rule	753
Creating Conditional Rules	756
Mapping Tables	756
About Data Generation Pattern Syntax	757
Dynamic Collections	758
Creating a Dynamic Collection	759
Filling out a Query Scope	759
Deleting a Dynamic Collection	761
Fields	761
Managing Fields	761
Required Fields	762
Unique Fields	763
Creating a Custom Field	763

Table of Contents

Updating a Field	766
Deleting a Field	766
About Fields	767
Forms and Views	767
Managing Forms and Views	767
Using the Create Identity Form	769
About Forms and Views	770
Resources and Connectors	771
Managing Resources	771
Creating a Resource	771
Deleting a Resource	773
Roles	773
Creating a Role	774
Updating a Role	775
Deleting a Role	775
Roles and Access	775
Scenarios without RBAC	776
Benefits of RBAC	776
Connecting to Secret Server Cloud	777
Adding Privileged Remote Access to Secret Server On Premises	777
Using Platform Integration Center	777
Overview	777
Integration Benefits	778
After Integration	778
Integration Steps	779
Step 1: Provision a Platform Tenant	779
Step 2: Secure Access	779
Step 3: Customize Branding	781
Step 4: Connect Domains	781
Step 5: Set up Federation	782
Step 6: Data Pre-check	782
Step 7: Complete the Integration	783
Using Opt In Integration	784
Automated Platform and Secret Server Cloud Integration	785
New Delinea Customers	785
Current Secret Server Customers	785
Logging in and Getting Started	789
Using Manual Integration	791
Retrieve the Platform Integration Credentials	791
Enable Platform Integration in Secret Server	792
Verify the Integration in the Platform	794
Verify the Integration in Secret Server	794
Link Platform and Secret Server Groups	795

Table of Contents

Synchronize Platform and Secret Server Groups	796
Connecting to Secret Server On Premise	796
Accessing the Delinea Platform	797
Prerequisites	797
Integration Steps	797
Install a Privileged Remote Access Engine	797
Add a New Secret Server Connection	797
Update the Platform Integration Settings On Secret Server	799
Update Your Secret Server Connection with the PRA Site	799
Verify the Overall Integration	800
Setting Up Resilient Secrets	800
Prerequisites	801
How Do Resilient Secrets Work?	801
Best Practices	802
Delinea Platform with Secret Server Cloud and Replica Secret Server Cloud	802
Delinea Platform with Secret Server Cloud and Replica Secret Server On-Premises	802
On-Premises Replica Authentication for Delinea Platform-Based Login	803
On-Premises Replica Authentication for Federation-based Login	803
On-Premises Source With Cloud Replica (SSC or Platform)	803
Frequently Asked Questions	803
Resilient Secrets Login Options	805
Server Suite on Delinea Platform	806
Release Notes	806
Please Wait...	806
Spring (Q2) 2025 Release	806
Secret Server on Platform	806
Continuous Identity Discovery (CID)	806
Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)	807
Analytics	807
Identity Lifecycle Management (ILM)	807
Privileged Remote Access (PRA)	808
Connection Manager (CM)	808
Inventory	808
Identity and Federation	808
Engine Management	809
Marketplace and Integrations	809
Other Updates	809
Winter (Q1) 2025 Release	810
Secret Server (SS) on Platform	810
Continuous Identity Discovery (CID)	810
Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)	811
Analytics	811
Privileged Remote Access (PRA)	811

Table of Contents

Connection Manager (CM)	812
Privilege Control for Servers (PCS)	812
Inventory	812
Identity & Federation	812
Engine Management	813
Marketplace & Integrations	813
Other Updates	814
Fall (Q4) 2024 Release	814
Secret Server (SS) on Platform	814
Continuous Identity Discovery (CID)	814
Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)	815
Snowflake Integration:	815
Privileged Remote Access (PRA)	815
Connection Manager (CM)	815
Privilege Control for Servers (PCS)	815
Identity and Federation	816
Platform Engine Management	816
Integrations and Marketplace	816
New Authenticator Mobile App	817
Other updates	817
Summer (Q3) 2024 Release	818
Secret Server on Platform	818
Remote Access Service (RAS)	818
Connection Manager (CM)	818
Identity & Federation	819
Audit	819
Permissions	819
Engine Management	820
Marketplace & Integrations	820
New Authenticator mobile app	820
Other updates	821
Spring (Q2) 2024 Release	821
Secret Server on Platform	821
Privileged Remote Access (PRA)	821
Connection Manager (CM)	821
Inventory	822
Audit	822
Marketplace & Integrations	822
Identity & Federation	823
Platform Engine Management	823
Privilege Control for Servers	823
Delinea Mobile App	823
Web Password Filler (WPF)	823
Other updates	824

Table of Contents

Winter (Q1) 2024 Release	824
Secret Server on Platform	824
Privileged Remote Access (PRA)	824
Connection Manager (CM)	825
Audit	825
Marketplace & Integrations	825
Identity & Federation	825
Other updates	825
Fall (Q4) 2023 Release	825
Secret Server on Platform	825
Privileged Remote Access (PRA)	826
Web Password Filler (WPF)	826
Connection Manager (CM)	826
Integrations and Marketplace	826
Identity & Federation	826
Other updates	827
Summer (Q3) 2023 Release	827
Secret Server on Platform	827
Privileged Remote Access (PRA)	827
Web Password Filler (WPF)	827
Connection Manager (CM)	827
Audit	828
Marketplace & Integrations	828
Identity & Federation	828
Other updates	829
Spring (Q2) 2023 Release	829
New Hosting Regions	829
Behavioral Analytics (Private Preview)	829
Permissions Service	830
Improved Home Screen	830
Marketplace	830
Tenant Customization	830
Winter (Q1) 2023 Release	830
Seamless Integration with Secret Server Cloud	830
Next-Gen Privileged Remote Access	831
Robust Identity and Federation Services	831
Marketplace	831
Foundational Shared Services	831
SMS Terms of Service	831
Local File Locations	831
Glossary	833

Introducing the Delinea Platform

The Delinea Platform represents a significant evolution in Privileged Access Management (PAM), offering a unified and comprehensive perspective on your organization's entire PAM ecosystem. Designed to extend Privileged Access Management seamlessly across hybrid multi-cloud infrastructures, the Delinea Platform introduces adaptive controls that empower IT and cybersecurity teams to secure credentials swiftly, minimize the attack surface, mitigate risks, and comply with regulatory requirements.

Benefits

The Delinea Platform delivers a multitude of benefits, including:

- **Decrease Risk:** Enhance your security posture by safeguarding privileged access from login to privilege elevation, and proactively address identity-related threats and misconfigurations.
- **More Easily Meet Compliance:** Adaptive authorization controls and unified auditing simplify the enforcement and demonstration of compliance requirements.
- **Centralize Control:** Manage privileged access across shared credentials and all identities spanning data, applications, cloud, and traditional infrastructure.
- **Scale Your PAM Program:** Leverage Delinea's secure cloud-native architecture to mature your organization through the seamless adoption of privilege controls and shared capabilities.
- **Realize Fast ROI:** Benefit from wizard-driven setup, configuration, and workflows that are easy to adopt.
- **Benefit from Cloud-Native Resilience:** Experience the most resilient solution, boasting 99.99% uptime.

Learn more about the [Delinea Platform](#) and its [shared service capabilities](#).

Secret Server

Protect your privileged accounts with Secret Server, our enterprise-grade Privileged Access Management (PAM) solution.

Robust Identity and Federation Services

- Support for OIDC and SAML federation.
- Support for Active Directory.
- Policy-based flexible MFA including Fido2, Email, SMS, etc.

Privileged Remote Access (formerly RAS)

- Launch secure VPN-less browser-based SSH and RDP sessions with a single click.
- Agentless deployment: no additional software is required on your target hosts.
- Agentless session recording through new auditing capabilities.

Table of Contents

- No end-user clients required: all based on a modern HTML5-based web client.
- Zero impact on customer security posture: no inbound firewall rules to open.
- Support for both Secret Server Cloud and On-premises deployments.

Privilege Control for Servers

- Apply zero trust and least privilege principles to prevent lateral movement while providing just-in-time and just-enough privileged access.
- Enforce Multi-Factor Authentication (MFA) at server log-in and privilege elevation for additional identity assurance.
- Harden privileges on Windows, Linux, and Unix servers across all identities that have direct server access for granular tracking and reporting.

Identity Threat Protection

- Discover identity misconfigurations and anomalous behavior across federated and local identities.
- Visualize identity access pathways across identity systems, SaaS applications, cloud, and traditional infrastructure.
- Highlight the danger and impact of identity-related threats and more efficiently know what to address.
- Take recommended actions or automate responses to reduce the impact of an attack.
- Deliver fast time-to-value and lower total cost of ownership with comprehensive identity security in the cloud-native Delinea Platform.

Privilege Control for Cloud Entitlements

- Right-size entitlements to limit risk but enable productivity.
- Find misconfigurations and normalize privileged behavior across the cloud.
- Find identities and their entitlements in constantly changing complex cloud environments.

Integrations and Marketplace

The Delinea Integrations and Marketplace is your one-stop shop for Delinea Platform add-on technologies, including Delinea applications, partner integrations, services, utilities, tools, scripts, and direct downloads.

NextGen Mobile Application

A new mobile app with support for the following:

- Simplified push notifications
- Updated, intuitive user interface
- Multi-factor authentication

Table of Contents

- Biometric unlock
- Autofill
- Use, create, download, organize secrets
- Offline access to secrets

To begin using the platform, proceed to the next section, "Quick Start Guide" below.

Near-Perfect Uptime

The Delinea Platform is setting a new bar for cloud-native identity security, delivering near-perfect uptime of **99.995%** by contractual Service Level Agreement (SLA).

Other vendors in this space say they offer 99.950% or 99.990% uptime, but these claims don't necessarily apply to contractual SLAs. And many vendors exclude scheduled maintenance as well as planned downtime for upgrades or customer-side misconfigurations. In practice, your service could be offline for over 170 minutes per year and still be considered "within SLA."

In contrast, Delinea is committed to the equivalent to **~26 minutes of allowable downtime annually**. That SLA includes situations like cloud provider outages and activities like upgrades and patching, which happen in Delinea without scheduled maintenance. It's nearly on par with the highest Tier IV data center standards (fully fault-tolerant systems).

Uptime: Delinea Platform vs. Legacy SaaS

	Legacy SaaS architecture	Delinea Platform architecture
Uptime	<= 99.950%	99.995%
Downtime during upgrades	15+ minutes	None
Scalability	Vertically with downtime Horizontal with configuration	Auto-scale vertically and horizontally
Code to production time	4+ weeks	30 minutes average




Note: The relevant Delinea SLA has been split in two:


- [Service Level Addendum for Delinea Platform](#) (described above)
- [Service Level Addendum for Delinea Cloud Services](#) (other than the Delinea Platform)

Quick Start Guide

This guide is for new or prospective Delinea customers who wish to purchase or sign up for a trial of the integrated Secret Server Cloud on the Delinea Platform, with **unified administration**. With unified administration, individual administrators can access both Secret Server Cloud and platform functionality simultaneously and seamlessly.

The guide is **not** for existing Secret Server Cloud or Secret Server On Premises customers. See the **Notes** below:

 **Note:** Existing Secret Server Cloud customers must integrate their Secret Server Cloud instance into the Delinea Platform. Please see "Connecting to Secret Server Cloud" on page 777.

 **Note:** Existing Secret Server On Premises customers can add Privileged Remote Access functionality using a limited integration. Please see "Connecting to Secret Server On Premise" on page 796.

To troubleshoot common on-boarding issues, see [Onboarding Troubleshooting](#).

The Cloudadmin Account


Delinea creates the cloudadmin account for you, with the name formatted as `cloudadmin@your_platform_tenant_name`. It is the first account on the platform, and it has unlimited permissions across the platform and Secret Server Cloud. When you are signed in as cloudadmin, you will perform initial provisioning, login, and setup tasks that include installing the Delinea Connector, authorizing domain user accounts, assigning your own business domain user account to the System Administrator group.

Other Administrator Accounts

After you create the Platform Admin account, you can create additional administrator accounts with permissions tailored to specific purposes.

Provision and Log In to the Platform

1. Contact a [Delinea sales representative](#) to request a trial platform account.

 **Note:** If you do not receive one or more of the following emails from Delinea, see [Onboarding Troubleshooting](#) for guidance.

2. **Welcome to your Secret Server Cloud Trial on the Delinea Platform:** You will receive this initial email when you are approved for a trial. Use the links in the email to provision your platform cloud tenant and perform these tasks:
 - Set up your platform cloud tenant
 - Set up your initial administrator account
 - Select your hosting region
 - Choose a subdomain for your organization
 - Receive your platform access licenses
 - Designate an alternate owner at your organization
 - Sign up for Delinea Support services
3. **Welcome to the Delinea Support Portal!** You will receive this second email after you complete the tasks in the first email. Click the link in this email to sign into your personalized Delinea Support portal with the username provided in the email.
4. **You have been invited to the tenant-name tenant on Delinea Platform:** You will receive this third email after you use the link in the second email to log in to the Delinea Support portal.

Table of Contents

- Make a note of your Cloudadmin account login username provided in the email.
- Click the **Accept Invitation** button in the email to be taken to your platform tenant, where you will be logged in automatically the first time, with comprehensive administrator permission on both the platform and Secret Server.
- Bookmark your platform tenant URL.
- The second time you log in, you will be prompted to set a password for your Cloudadmin account. We recommend having this password generated for you automatically.



Note: Not all platform features are available by default. To trial features like ITP/PCCE or PCS, contact your sales representative to have these enabled in your tenant.

Enable Domain Users to Log into the Platform

To enable domain users to log in to the platform, you must "Install the Delinea Connector and Authorize AD Accounts" below or configure Federation to "Add Federated User Accounts" on the next page, or you use both options for a mix of user types. You can then define security policies, assign them to platform identity groups, and map your existing domain groups to the platform identity groups.

Install the Delinea Connector and Authorize AD Accounts

To add Active Directory user accounts to the platform, you must install the Delinea Connector. For complete instructions on downloading, installing, and registering the Connector, see [Delinea Connector](#).

The basic steps for installing the Delinea Connector are as follows.

1. Download the connector executable file by clicking **Settings** from the left navigation, then selecting **Connectors**.
2. On the Connectors page, click **Add Connector**.
3. In Box 1 on the Add connector page, click **Download** to get the 64-bit Connector Installer.
4. In Box 2, copy the tenant URL, and save it for later.
5. Generate or copy a connector Registration Code, and save that for later too.
6. In the Connector Configuration Wizard, select the box next to **Use Registration Code** and paste the code that you saved earlier into the field provided. The Connector Configuration Wizard, similar to a Distributed Engine in Secret Server, will read the forest and automatically display a list of forest domains that you can connect to the platform.
7. Select any domain where your users will be logging in from.
8. Make sure to include the domain that your own business user account belongs to.

To map Microsoft Entra ID groups to platform groups, see [Integrating Entra ID](#).

Assign Your Business Domain User to the System Administrator Group

After you have authorized Active Directory accounts on the platform, including your own personal domain account, you need to assign standard Administrator permissions for platform and Secret Server to your personal domain account, while logged in as cloudadmin.

Table of Contents

1. Click **Access** from the left navigation, then select **Groups**.
2. Click the **System Administrator** group.
3. Click the **Members** tab.
4. Click **Add members**.
5. In the Search dialog, change the first filter to **Users** and change the second filter to your connected domain. Now the search will find users from your connected domains.
6. Find your own Platform Admin domain account and add it to the **System Administrator** group. Through your membership in this group, your account automatically inherits the **Platform Admin** role with appropriate permissions on the platform.

Synchronize the System Administrator Group to Secret Server

1. Click **Settings** from the left navigation, then select **Administration** below Secret Server.
2. On the Secrets Administration page, click **Platform Integration**.
3. Select the **Groups** tab.
4. Add the platform System Administrator group to the list of synchronized groups. Secret Server automatically creates a corresponding Secret Server group that is synchronized to the platform group.
5. Add a role with Secret Server administrator permissions to the new enabled platform System Administrator group. Your platform System Administrator account now has Secret Server administrator permissions through its membership in the synchronized Secret Server group.

Access Secrets as a System Administrator

After you have assigned your business domain user to the system administrator group and synchronized the system administrator group to a secret server, you can access secrets from the platform using your System Administrator account.

1. Log out of the platform as Cloudadmin.
2. Log back into the platform using your System Administrator account.
3. On the platform Home page, click **Access Your Secret Server**. The All Secrets page opens, where you can view, create, and manage your secrets.

For more on how to use and manage your secrets, see [Using Secrets](#).

Add Federated User Accounts

Unlike Secret Server Cloud users, federated Delinea Platform users are added to the platform "on-the-fly" when they log in, as long as they satisfy the authentication requirements through an external source such as AD or a federation service provider. Users do not need to be authorized or granted permissions in advance. Users that exist in external sources will not be listed on the platform at **Access >Users** until they log in to the platform for the first time.


The platform does not natively support bulk import and synchronization of all users from an external source such as federation or AD. Platform administrators can find AD users to add to the platform by performing filtered searches through external AD directories, but federated directories cannot be searched.


To integrate federation Identity Provider (IdP) services on the Delinea Platform, see [Federation](#).

To manage federation IdP services on the platform, see [Federation Management](#). Also see [Troubleshooting Federated User and Group Mapping](#).

About Local User Accounts

Adding local users to the platform is not considered a best practice for privileged access management. Generally, users should be added to the platform only through federation or through their membership in an Active Directory. Local user accounts should be used **only rarely**. For example vendors are added as local accounts, and you might need to add a local user account for someone who needs to try out platform functionality for a very limited time.

 **Note:** Local accounts cannot be converted to domain accounts.

 **Note:** (for migration customers only) After the Connector is installed and Active Directory is set up on the platform, do not add an existing Secret Server Cloud user as a local user, because doing so could cause synchronization issues between the platform and Secret Server.

To add a new local user, see [Adding Users](#).

Assign Roles and Permissions to Users and Groups

On the Delinea Platform, permissions are assigned to roles, and roles are assigned to groups, so users inherit permissions through their group memberships. The platform supports custom roles and the following two built-in roles, which cannot be renamed or deleted:

- **Platform User:** All platform users belong to the Everybody group, and through that group membership they inherit the Platform User role. The Platform User role provides the user with basic permissions to log in to the platform, access their secrets, launch PRA sessions, and view their own session recordings.
- **Platform Admin:** Platform users added to the System Administrator group inherit the Platform Admin role through that group membership. The Platform Admin role provides all permissions on the platform.


User roles and permissions are managed by clicking **Access** from the left navigation, then selecting **Users**, **Groups**, or **Roles**.

For more detailed instructions on managing roles and permissions on the platform, see [User Roles and Permissions](#).

Set Up and Use Privileged Remote Access

Delinea Privileged Remote Access (PRA) provides seamless access to remote machines through Remote Desktop Protocol (RDP) and Secure Socket Shell (SSH), with no need for a Virtual Private Network (VPN).

Install the Remote Access Engine

 **Note:** Before you install the PRA engine, make sure you meet the minimum requirements. See [PRA Requirements](#).

1. Click **Settings** from the left navigation menu, then select **Remote Access**.
2. Click **Add Site**.
3. Follow the instructions at [Create a Site](#).

4. Follow the instructions at [Install an Engine](#).
5. Follow the instructions at [Activate the Engine](#).

Launch a PRA Session

To launch a PRA session from the Delinea Platform:

1. From the left navigation menu, click **Secret Server**.
2. On the All secrets page, locate a secret associated with PRA.
3. Hover your cursor near the right end of the **Name** field.
4. Click the rocket (launch) icon. The Select Launcher window pops up.
5. Select **Open with Remote Access**. A new browser tab opens, where you can launch a PRA connection to a remote machine.

For more detailed instructions on using the Privileged Remote Access, see [Using the PRA Engine \(Deprecated\)](#).

Set Up Continuous Identity Discovery

Continuous Identity Discovery (CID) continuously identifies privileged cloud service users that are not yet vaulted in Secret Server Cloud. We recommend vaulting these accounts in Secret Server to enforce proper login, or disabling the user if access is unnecessary.

To discover privileged accounts not managed in Secret Server, select **Identity Posture > Checks** and review the following checks:

- **Unvaulted Admin Credentials**
Discover cloud service administrators whose credentials are not in Secret Server.
- **Unvaulted Shadow Admin Credentials (for CSP only)**
Discover cloud service [shadow admins](#) whose credentials are not in Secret Server.
- **Unvaulted Privileged Account Credentials**
Discover privileged cloud service user accounts whose credentials are not in Secret Server.
- **Unvaulted Admin Access Keys (for AWS only)**
Discover cloud service administrators whose access keys are not in Secret Server.
- **Unvaulted Shadow Admin Access Keys (for AWS only)**
Discover cloud service [shadow admins](#) whose access keys are not in Secret Server.
- **Unvaulted Privileged Account Access Keys (for AWS only)**
Discover privileged cloud service user accounts whose access keys are not in Secret Server.

For details, see [Continuous Identity Discovery](#).

About Multi-factor Authentication

The platform provides cloud-based, flexible multi-factor authentication (MFA) as powerful as many retail MFA products and services. All administrators and business users on the platform should be required to use multi-factor authentication (MFA) to log in.

Platform MFA has two components: Authentication Profiles and Identity Policies.

Table of Contents

- An identity MFA *profile* determines which MFA challenges are presented to a user (see [Authentication Profiles](#)).
- An identity MFA *policy* determines whether and when a user is presented with the challenges in their assigned MFA profile (see [Identity Policies](#)).

More information about MFA on the platform can be found in the following sections:

- [MFA for Secrets](#). Multi-factor authentication (MFA) for secrets gives platform administrators the option to add one or more security requirements to access defined secrets.
- [Identity Policies](#). Enabling MFA on the platform requires setting up identity policies and assigning them to users. An identity policy determines whether and when a user is presented with the challenges specified in the associated MFA profile.
- [Authentication Profiles](#). Enabling MFA on the platform requires setting up authentication profiles. An authentication profile specifies the authentication challenges required to log in to the platform, and the length of time that must elapse before a user is re-prompted for authentication.
- [Corporate IP Range](#). The Corporate IP Range function is used to define IP ranges for both internal and external networks, and to define authentication requirements such as the locations or IP ranges from which users can log in to the Delinea Platform.
- [RADIUS Authentication](#). You can use your RADIUS server to authenticate users to the Delinea Platform.
- [Logging In to the Delinea Platform \(MFA\)](#). The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. Also see [Delinea Mobile Log in Process](#).

Delinea Platform Interface

The platform's user interface is designed to make all platform functions highly visible and readily accessible.



Note: Most features that were previously under Administration now appear under Settings.

Primary Left Navigation Menu

The options available in the left navigation menu vary depending on the services you subscribe to.

- **Home:** Set up your platform, open your applications, and browse learning resources
- **Secret Server:** See your secrets in various categories: all, favorites, most used, recently used, quick access, and recent folders
- **Inventory:** See and manage every computer in your network at a glance
- **Insights:** Session review, audit logs, Secret Server reporting, and session recording
- **Discovery:** Charts and logs about your platform environment
- **Policies:** Fast access to all privilege control policies
- **Identity Posture:** Monitor the status of all applications compared to best practices
- **Threat Center:** Configure rules to detect threats that trigger administrator actions
- **Access:** Manage users, groups, roles, and identity policies
- **Marketplace:** A one-stop shop for applications, integrations, downloads

Table of Contents

- **Inbox:** Notifications, system alerts, and requests
- **Settings:** Administrator controls for platform setup, Secret Server, connection points, directory integrations, MFA, and security

Secondary Navigation |

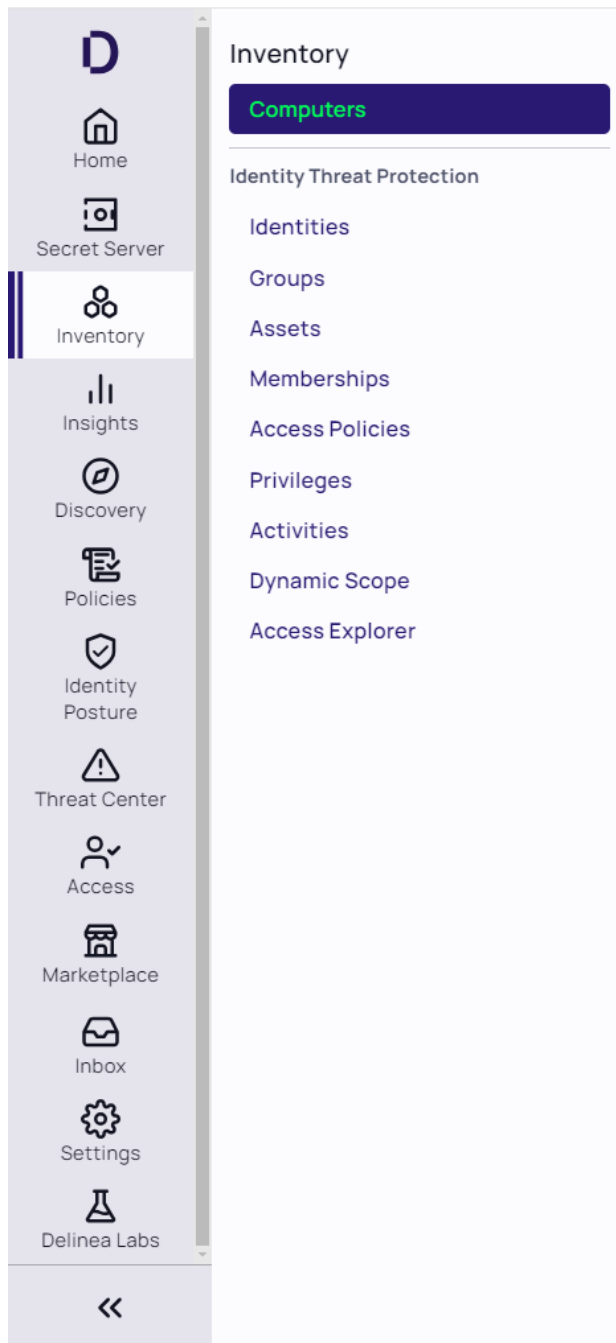
The secondary navigation menu slides out to the right, providing access to all functions relevant to the primary navigation item. This provides quick access with less searching and fewer clicks.

Hover over a menu item

When you hover over a primary navigation menu item, the secondary navigation slides out, instantly displaying all functions related to the primary menu item. When you move your cursor away, the secondary menu slides back

Table of Contents

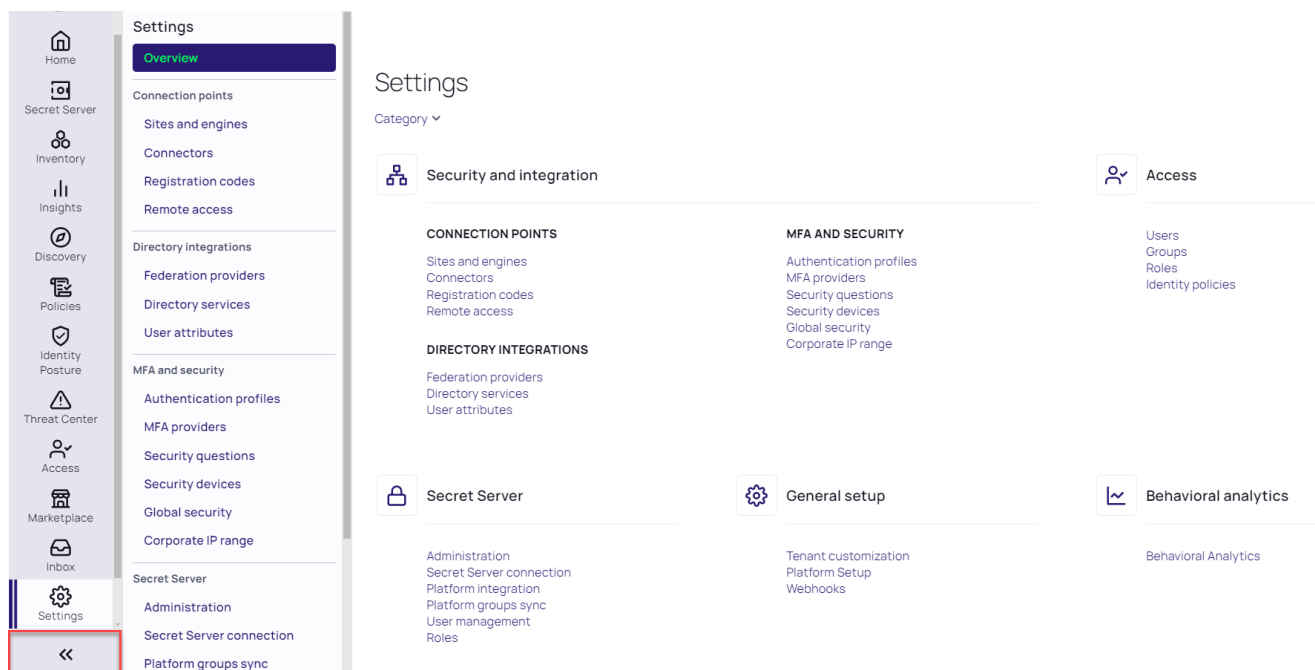
behind the primary menu.



Click a menu item

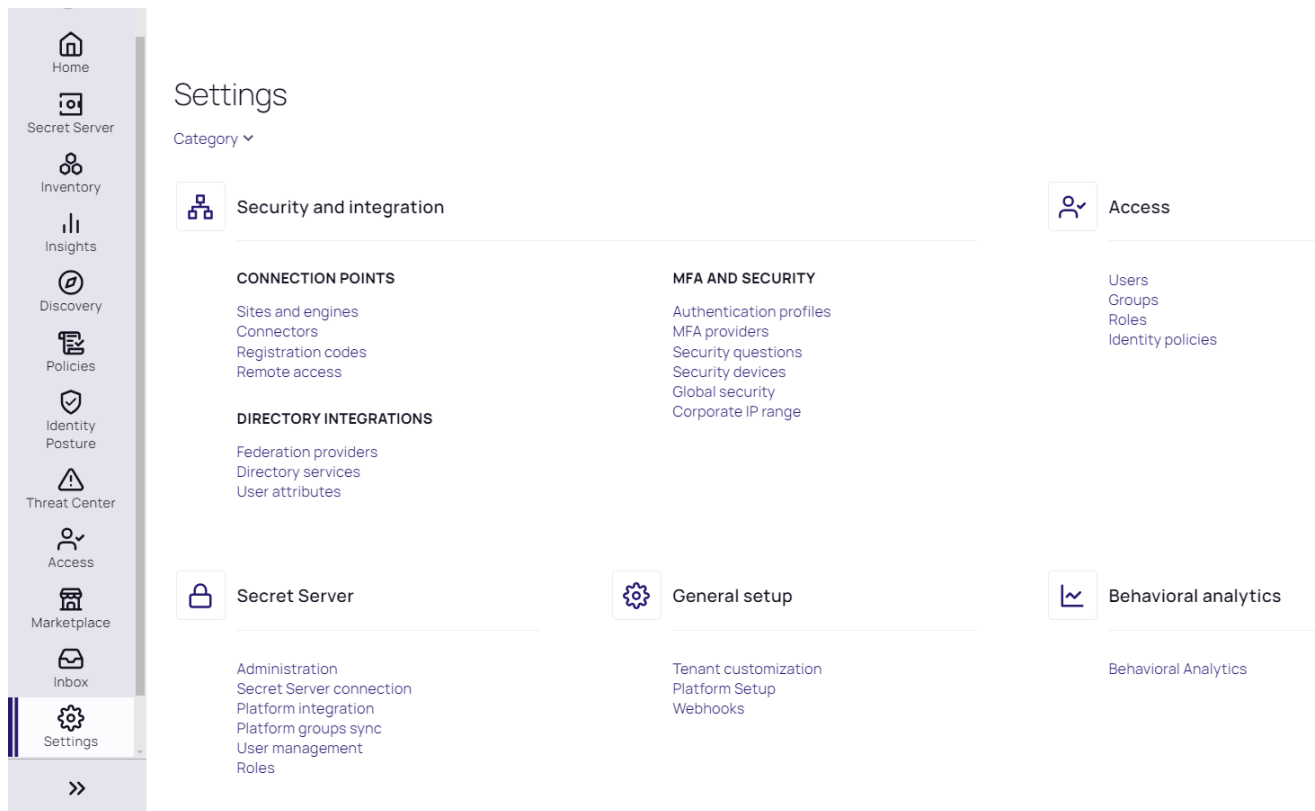
When you click a primary menu item, two things happen. First, the secondary menu slides out and remains open, even if you move your cursor away. Second, the page associated with the top item on the secondary menu opens automatically to the right.

Table of Contents



Once you've found the page you're looking for, you might not need to see the secondary menu anymore. To give you more room to see the page, click the expansion control at the bottom of the left navigation menu to slide the secondary menu back under the primary menu.

Secondary Menu Collapsed



Global Search

The platform Search bar returns results for all relevant areas of functionality and to specific items across the platform including secrets, assets, folders, and individual configuration items. When you enter a search term, a toggle button (solid purple) appears for each relevant area of functionality.

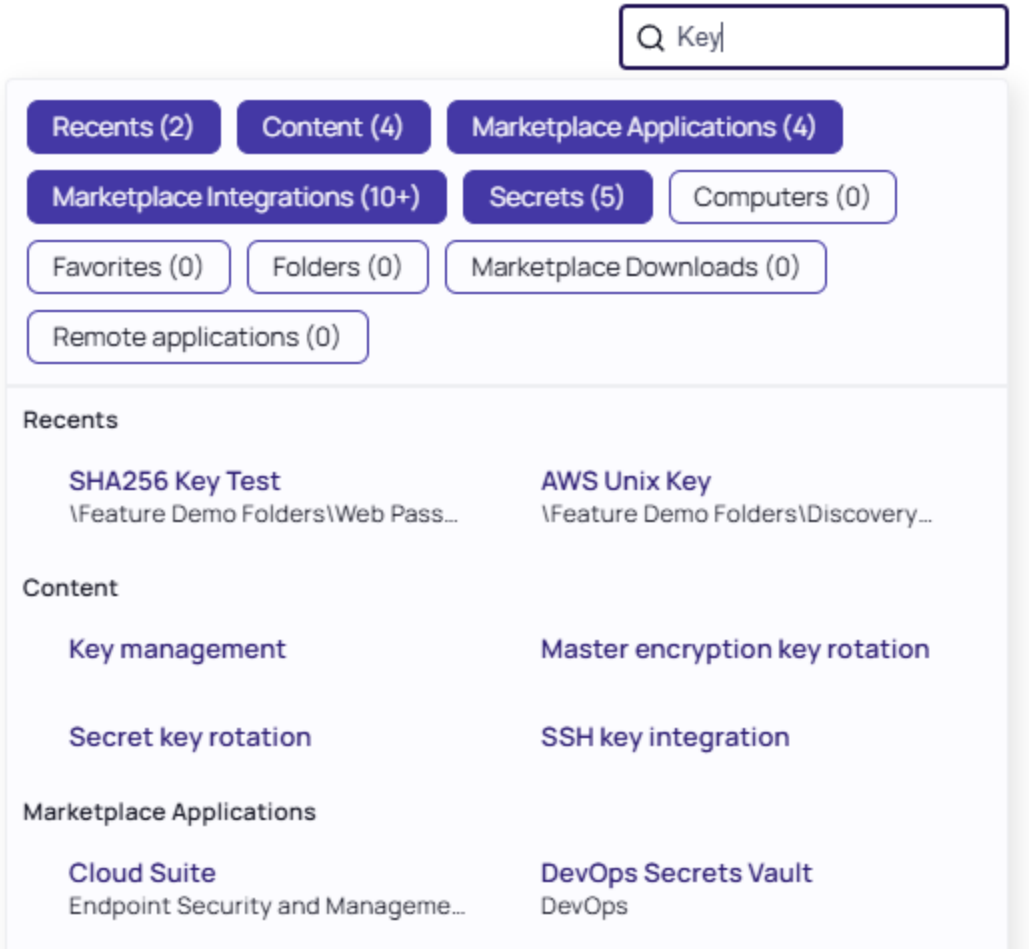
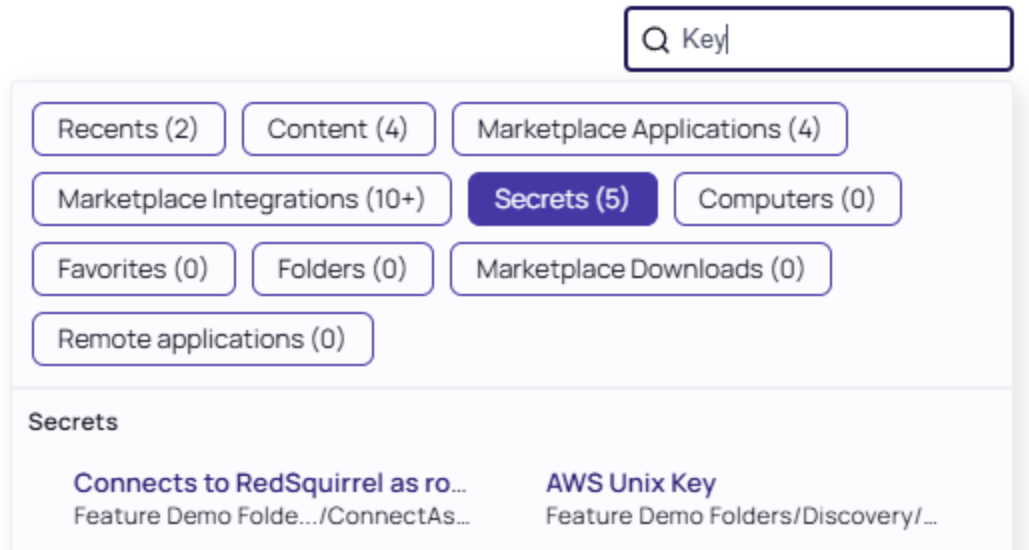



Table of Contents

By clicking one or more toggle buttons (Secrets in the screen shot below) you can limit your search to those areas of functionality. This feature is especially helpful when multiple functions share a similar name.



Some context-sensitive actions such as launching can be executed directly from the search results.

Favorites and Recents

 **Note:** This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

Favorites

You can mark all platform configuration pages and most details pages as Favorites by selecting the star icon at the top of the page. Your favorite pages will be indexed for search, providing fast access to those pages.

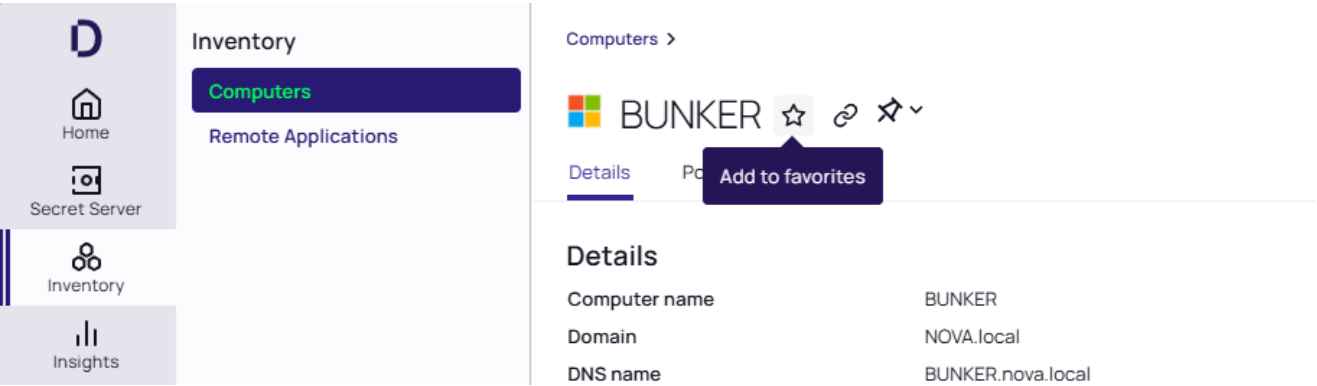


Table of Contents

You can then access your favorited pages by clicking **Home > Favorites**.

The screenshot shows the Delinea Platform user interface. On the left is a sidebar with icons for Home, Secret Server, Inventory, Insights, and Discovery. The main content area is titled 'Favorites' and contains a search bar, filter buttons for 'Type' (All types) and 'Date added' (All time), and a table of 7 items. The table has columns for NAME, TYPE, and DATE ADDED. The items listed are 'Computers' (Page, 3 months, 26 Days ago) and 'MFA Demo' (Secret, 1 year, 2 months ago).

NAME ↑	TYPE	DATE ADDED
★ Computers	Page	3 months, 26 Days ago
★ MFA Demo	Secret	1 year, 2 months ago

Recents

To access your recently-visited pages, click **Home > Recents**.

The screenshot shows the Delinea Platform user interface. On the left is a sidebar with icons for Home, Secret Server, Inventory, Insights, Discovery, Policies, and a checkmark icon. The main content area is titled 'Recents' and contains a search bar, filter buttons for 'Type' (All types) and 'Date added' (All time), and a table of 33 items. The table has columns for NAME, TYPE, and LAST ACCESSED. The items listed are 'Engine management' (Page, 1 hour, 33 Minutes ago), 'Overview' (Page, 1 hour, 33 Minutes ago), 'Federation providers' (Page, 3 Days, 1 hour ago), 'Groups' (Page, 3 Days, 1 hour ago), and 'Users' (Page, 3 Days, 1 hour ago).

NAME	TYPE	LAST ACCESSED ↓
Engine management	Page	1 hour, 33 Minutes ago
Overview	Page	1 hour, 33 Minutes ago
Federation providers	Page	3 Days, 1 hour ago
Groups	Page	3 Days, 1 hour ago
Users	Page	3 Days, 1 hour ago

Filtering in List Pages

Many of the pages in the Delinea Platform user interface are list pages, which display a table that lists some type of objects in the platform; for example, the Computers page in the Inventory part of the user interface. By default, each list page includes a table displaying all data relevant to the page.

The list pages offer various types of filtering, depending on which page you are viewing:

- Some list pages, such as the Collections page in the Inventories part of the user interface, have only a Search box at the top of the list. You can type a name to find one of the items in the list.
- In most list pages, in addition to the Search box, you can also filter the table based on the properties of the listed objects. For example, in the Policies page, you can filter for policies that match based on both user (Subject) and target computer. See ["Using Quick Filters" on the next page](#).

Table of Contents

- In some pages, such as the Computers page in the Inventory part of the user interface, you can use a query builder to construct more sophisticated filters. With the query builder, you can filter a table based on a broader set of properties and interconnected relationships. See ["Using the Query Builder"](#) below.

Using Quick Filters

In most list pages, you can choose among predefined quick filters that are commonly used for that list.

To filter a table:

- To add filter fields, click **Add filter** and select from the available filter fields. (If **Add filter** does not appear, all the available filter fields are already selected.)
- To remove fields, hover over a field and click **X**.

As you make each change to the filter fields, the displayed table is modified to match the new filter criteria.

If you have imported custom properties (shown at the end of the list), you can use them to filter. For more information on importing custom properties, see ["Searching by Custom Properties"](#) on page 681.

If you filter on a type of entity that can be grouped, the filter finds the entity within the group. For example, if User is selected, the filter finds the user in all user groups as well as individually. If Computer is selected, the filter finds the computer even if it's inside a collection.

Using the Query Builder

In some pages, such as the Computers inventory page, you can use a query builder to filter a table based on a broader set of properties and interconnected relationships.

1. To open the query builder, click **Show query builder**.



Note: If this button is not visible, the query builder is not available in the page you are viewing.

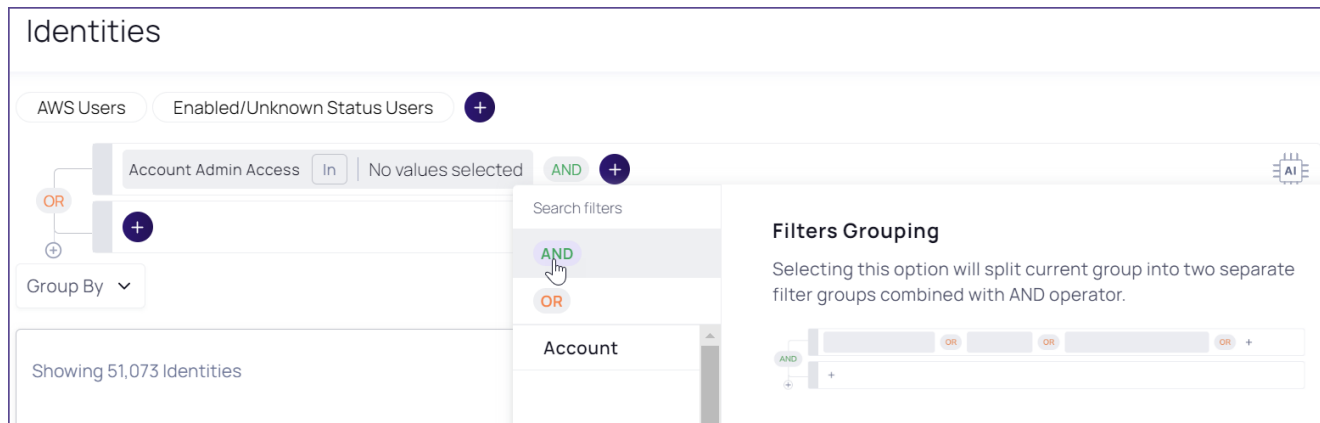
2. Click the plus icon (+) to add a filter field to the query. For example, select Computer Type.
3. If you want to change the operand for the filter, click **In** and select a different operand from the dropdown list. For example, to exclude rather than include items that match the selected Computer Type, change the operand to Not In.
4. Keep repeating these steps to add more filter fields to the query. Each time you add a filter, you can change AND to OR.

As you make each change to the query, the displayed table is modified to match the new criteria.

In the query builder, filter lines are connected by all AND operators or by all OR operators.

To split the current filter group into separate groups (to write more complex queries), click + and select AND or OR. To remove a filter group, hover and click X.

Table of Contents



When there are options within a filter (for example, which apps an account can access), those options are always connected by OR.

In the query builder, you can use the following operands for each filter field:

- Exact matches:
 - In or Not In
 - Is Empty
- Mathematical matches:
 - Equal to, Greater than, and so on
- Date matches:
 - Yesterday, Last Week, Last Year, and so on
- String matches:
 - Contains or Not contains
 - Ends with or Not Ends with
 - Starts with or Not Starts with

Release Notes

- [Change Log](#)
- [Spring \(Q2\) 2025 Release](#)
- [Winter \(Q1\) 2025 Release](#)
- [Fall \(Q4\) 2024 Release](#)
- [Summer \(Q3\) 2024 Release](#)
- [Spring \(Q2\) 2024 Release](#)
- [Winter \(Q1\) 2024 Release](#)
- "Fall (Q4) 2023 Release" on page 825
- "Summer (Q3) 2023 Release" on page 827

- [Spring \(Q2\) 2023 Release](#)
- [Winter \(Q1\) 2023 Release](#)

Please Wait...

Spring (Q2) 2025 Release

Secret Server on Platform

Azure Key Vault (AKV) Integration (in GA): Streamline secret and Non-Human Identity management with native integration to Azure Key Vault. This enhancement enables centralized secret updates, supports frequent rotation, and enforces governance with fine-grained roles, permissions, and full audit logging. Learn more about this capability [here](#).

Continuous Identity Discovery (CID)

Active Directory (AD) Support for CID (in GA): CID now supports Active Directory environments. Key features include:

- Discovery of privileged users (including admin, shadow, and other elevated accounts) through ACL-based permission analysis
- Enhanced AD visibility with the ability to view and filter directory data for easier investigation and management
- Learn more about this capability [here](#).

Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)

Google Cloud Platform (GCP) support for ITP (in GA): You can now integrate GCP with the Delinea Platform (ITP) to extend identity-centric security across your Google environment. This integration enhances access management and helps secure privileged identities by providing visibility into the following:

- GCP Role Refactor - Identify unused permissions within GCP roles to help you move toward a least privilege model.
- GCP Shadow Admin Check - detect shadow admins, non admin users with the ability to escalate their access to administrative
- Identify Non-Vaulted Accounts - Gain visibility into privileged, admin, and shadow accounts that aren't properly vaulted.
- Non-Rotated Access Keys - Identify and address non-rotated keys to ensure your security practices align with best practices for key management.
- Visibility - Identify and query users' access in workspace admin directory and GCP to explore their access per project
- Learn more about this capability [here](#).

Account MFA Factors (in GA): Organizations often struggle with limited visibility into the Multi-Factor Authentication (MFA) factors enabled across their cloud environments. With the general availability of Account MFA Factors, customers can now gain insights into the MFA methods enabled and their security level, quickly identifying high-risk users with weak authentication factors. Learn more about this update [here](#).

Analytics

Analytics Now (in Public Preview): Analytics provides deeper visibility into user behavior and risk, helping organizations strengthen their security posture. Key features include the following:

- Real-time risk scoring based on behavior and authentication threats
- Detection of anomalies and behavioral changes
- Near real-time threat investigation and response
- Customizable risk parameters to reduce false alerts and align with your policies
- Learn more about this new service [here](#).

Identity Lifecycle Management (ILM)

Identity Lifecycle Management (ILM) (in Private Preview): ILM streamlines the entire user identity lifecycle—from onboarding to offboarding—by dynamically adjusting access as roles evolve. Key features include the following:

- Automated Joiner-Mover-Leaver Processes: Seamlessly create and manage identities, provision access at onboarding, and adjust or revoke access as users change roles or exit.
- Security & Compliance: Built on the cloud-native Delinea Platform, ILM leverages real-time identity and access context to detect risk, enforce policies, and manage access automatically.
- Intuitive Workflow Design: Easily configure lifecycle workflows with a no-code, drag-and-drop interface—no custom coding required.
- Learn more about this new service [here](#).

Privileged Remote Access (PRA)

PRA Workloads (in GA): PRA capabilities are now available through a unified deployment on the Delinea Platform Engine, with centralized management via the Engine Management interface. This is supported on both Windows and Linux. As part of this change, PRA no longer supports the creation of new Sites or the installation of new Engines for standalone PRA engine. Tenants requiring new Sites or Engines must now use Platform Sites and deploy Platform Engines with PRA capabilities. Note that previously deployed PRA sites and standalone engines will continue to function normally but will not be updated to support new functionality on the future roadmap. Learn more about this new capability [here](#).

Connection Manager (CM)

Connection Manager 2.6 Release

- External Browser MFA for Secrets: This update extends external browser-based MFA to protect access to secrets, adding a new layer of security through the Delinea Platform. Previously, this MFA method only supported platform login.
- Fullscreen Display Support for macOS: Users on macOS can now enjoy a more seamless and native full screen experience in CM, enhancing overall usability.
- New SSH Terminal for macOS: A redesigned SSH terminal delivers improved performance, user experience,

Table of Contents

and convenience for macOS users.

- More updates and enhancements are detailed in these [release notes](#).

Connection Manager 2.6.1 Release

- This release addressed a couple bug fixes and their related improvements. See [release notes](#) for additional details.

Inventory

Permissions on Collections (in Public Preview): You can now assign granular permissions to computer collections, allowing precise control over which computers end users can view and interact with. This new capability currently supports computer collections, with plans to extend to additional asset types in the future. This update also introduces a new permission specifically for launching access with Privileged Remote Access (PRA), along with UX enhancements to streamline the setup and management of these permissions. Learn more about this new capability [here](#).

Identity and Federation

Non-Interactive Service User Option (in GA): To help customers enforce the intended use of service users—automation, not interactive access—we've introduced a new non-interactive option in identity policies. When enabled, this setting prevents service users from logging in through the UI, reducing the risk of misuse and strengthening overall security. Interactive login remains available when needed, but customers now have full control over how service users can access the platform. Learn more about this update [here](#).

Engine Management

Enhanced Web Proxy Support for Deployments (in GA): This update addresses issues where restrictive web proxy settings block configuration file downloads, leading to deployment failures. We've introduced improved proxy handling across Engine binary download, configuration file retrieval and engine service communication. Learn more about these updates [here](#).

Marketplace and Integrations

View Configured Integrations: Added the ability to view all configured integrations, providing greater transparency and easier management. Learn more about this update [here](#).

Download Center UX Improvements: Improved usability in the Download Center for a more streamlined and intuitive experience. Learn more about the Download Center [here](#).

New and Updated Integrations:

- CrowdStrike Falcon Fusion SOAR Integration GA
- Addition of GitGuardian Scout Integrations for Delinea Platform GA
- Keyfactor Control Integration GA
- Avantra AIOPs for SAP for Delinea Platform GA
- RabbitMQ Helper 12.1.0
- Oracle JDBC Proxy Driver to support Delinea Platform

Table of Contents

- Rapid7 InsightVM with Delinea Platform
- Integration with ConnectWise Screen Connect V4.0 to support Delinea Platform
- External Secrets K8 Integration
- Utimaco support for u.trust General Purpose HSM Se-Series

Other Updates

United Arab Emirates (UAE) databoundary availability: Customers with data residency requirements in the UAE and neighboring regions can now deploy the Delinea Platform and Secret Server Cloud within the UAE. This new regional deployment offers reduced latency and enhanced performance for customers in this region. Learn more about regional availability [here](#).

Delinea Platform Mobile App: Vaulting capabilities are now available in the Delinea Platform Mobile app, expanding on the existing mobile features to deliver a more complete, end-to-end experience for users managing the platform on the go. This update empowers users with greater control and flexibility, even when away from their workstation.

- Create and edit Secrets directly from the mobile app
- Complete security workflows on the move
- Access vaulted credentials securely from your mobile device

Improved Grid Filter Persistence for Seamless Task Switching: We've made it easier to pick up where you left off. Full-page grids can now remember your filter settings between sessions, reducing time spent reapplying filters when returning to previous tasks. Turn on the "Remember filter values" option under User Preferences in Platform to start using this feature.

Secret Icons for a More Intuitive Experience: Icons can now be associated with Secret Templates to make it easier for users to visually identify and interact with different types of secrets. Learn more about this update [here](#).

Performance and Resiliency Enhancements for Policy Propagation: Several improvements added to ensure smoother and more reliable policy propagation for Privilege Control for servers, especially in environments with a high volume of policies. Key updates include the following:

- Enhanced resiliency for Command Relay under load
- Optimizations to messaging queue handling for better throughput and stability
- Improved processing efficiency for collections, reducing latency and improving scalability

Winter (Q1) 2025 Release

Secret Server (SS) on Platform

- **Platform Integration Center** (in private preview): Designed to provide a path for existing Secret Server Cloud tenants to fully integrate with the platform, from standalone tenants through to fully unified. Learn more about this update [here](#).
- **Event-Driven User and Mapping Updates:** Secret Server now supports near-real time updates for user mapping changes through event-driven processing.
- **Entra ID Discovery Enhancements:**

Table of Contents

- **Account Type Filtering:** Added the ability to filter Entra ID account types during Discovery, including options to exclude External Accounts and Synchronized On-Premises AD Accounts.
- **Heartbeat and MFA Enrollment:** Heartbeat checks now support accounts pending MFA enrollment, with improved error handling for reliability.
- **Role Assignments via Groups:** Entra ID Discovery now identifies role members assigned through group memberships.
- **Improved Search Performance:**
 - Resolved performance issues during secret searches by optimizing internal logic to limit searches to user-accessible secrets.
 - Enhanced database handling by eliminating deadlocks and significantly improving performance.

Continuous Identity Discovery (CID)



Note: Continuous Identity Discovery was previously referred to in Delinea Platform as Continuous Identity Discovery.

- Continuous Identity Discovery (CID) (in GA) helps discover privileged cloud identities, including admins, shadow admins, and privileged non-human identities that are not vaulted in Secret Server and suggest vaulting them in a click of a button. Learn more about this new service [here](#).
 - **Continuous, Out-of-the-Box Discovery:** Discover privileged accounts, including shadow admins, admins, and both local and federated accounts, without the need for custom scripts.
 - **Detect PAM Bypassing:** Identify users accessing cloud applications directly, bypassing the vault.

Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)

- **Workday integration** (in GA) - leverage Workday as a source of truth for better visibility and posture.
 - Gain a comprehensive view of your workforce with enriched identity-level information.
 - Use Workday as a trusted source-of-truth to discover partially off-boarded users and external accounts.
 - Enhance identity merging by leveraging diverse account properties like email and employee ID.

Learn more about this new integration [here](#).

- **Introducing Cases** (in GA): Incidents are being replaced with a new layer for security findings in ITP and PCCE, designed to reduce noise by grouping alerts based on predefined logic, such as attack patterns or entities. Cases are now the central location for customers to access actionable, security-relevant items. Learn more about this update [here](#).

Analytics

- **Introducing Analytics** (in Private Preview), enabling organizations to gain deeper insights into user behavior and risks while maintaining their security posture.
- **Know Your User Risk:** Monitor and identify your riskiest users with automatically calculated risk scores based on behavioral patterns and authentication threats, making it easy to spot anomalies.

Table of Contents

- **Recognize Behavioral Change:** Detect deviations from normal activity, with baseline behavioral indicators so you can identify and respond to potential threats with efficiency and precision.
- **Proactively Protect Accounts:** Protect all accounts from attacks by recognizing when there is a potential threat in progress and investigate in near real-time before they get in and cause damage.
- **Customize Risk Parameters:** Adjust scoring weights and alert thresholds to align with your organization's specific needs. Customization is key to making security work for you by ensuring you set the rules to avoid false alerts and irrelevant workflows.

Learn more about this new service [here](#).

Privileged Remote Access (PRA)

- **PRA Workloads** (in Public Preview): Unified deployment of PRA capabilities on the Delinea Platform Engine and a centralized Engine Management interface. Available for both Windows and Linux. Learn more about this new capability [here](#).
- **Kerberos Support** (in GA): PRA users can now securely access target machines within Windows Domains that utilize Kerberos authentication.
 - **Enhanced Security:** Kerberos mitigates risks associated with NTLM, including Pass-the-Hash, DC Sync, NTLM-relay, and other attack techniques. Refer to Microsoft's NTLM deprecation announcement for more details.
 - **Seamless Integration:** For customers using both Kerberos and NTLM, the "fall back to NTLM if Kerberos fails" approach ensures uninterrupted access and flexibility. Learn more about this update [here](#).
- **New Disconnect Remote App Session:** A new Ctrl+Alt+Delete shortcut added to the Disconnect menu in PRA to prompt users to sign out from their session. Learn more about this update [here](#).

Connection Manager (CM)

- **Connection Manager 2.5.4 Release**
 - **Simplified Authentication Flow:** Users can now authenticate to Secret Server via an external browser without needing to click on a Secret Server page to launch Connection Manager.
 - **Preconfigured Vaults for Administrators:** Administrators can preconfigure multiple vaults, eliminating the need for users to create connections when opening Connection Manager for the first time.
 - **Additional Updates:** More updates and enhancements are detailed in these [release notes](#).

Privilege Control for Servers (PCS)

- **Run As Service Account or Domain Group.** This feature is part of the Granular Commands capability (in GA) allows applications to run as an Active Directory user or domain group, eliminating the need to log in as a specific user to complete tasks. Learn more about this new capability [here](#).
- **Multi-Factor Authentication (MFA) for Server Suite** (in GA). Server Suite customers can now integrate with the Delinea Platform as an MFA source. Learn more about this new capability [here](#).

Inventory

- **Collections** (now in GA): This new capability allows computers to be grouped by shared attributes for easier management. Policies can now be streamlined and applied to collections, minimizing manual effort. Additionally, collections automatically update as new computers meet the defined criteria, enhancing scalability and ensuring that asset management remains efficient as the environment grows. Learn more about this new capability [here](#).
- **Permissions on Collections** (in Private Preview): You can now assign detailed permissions to computer collections, controlling which computers an end user can view and interact with. This capability currently applies to computer collections, with more asset types to be added in the future. Learn more about this new capability [here](#).

Identity & Federation

- **Enhanced Security with Duo Integration** (now in GA): Customers can enable Duo MFA for an extra layer of security during login and authentication, strengthening their security posture while ensuring a seamless user experience. Learn more about this new integration [here](#).
- **Native Entra ID Integration** (in Private Preview): The Delinea Platform introduces a direct API integration with Microsoft Entra ID, offering seamless SSO login and MFA using Entra ID credentials. This integration enables direct usage of Entra ID groups without the need for local mapping or user claim mapping. It also provides a streamlined experience for browsing Entra ID groups and users within the platform, while supporting the pre-assignment of users to roles and permissions prior to their first login. Learn more about this integration [here](#).
- **Federation Automated Group Mapping** (in Private Preview): This feature dynamically creates and assigns groups based on group claims received from the IdP during user authentication, eliminating the need for manual configuration. This enhancement saves time, reduces effort, and minimizes the risk of human error when group mapping at scale. Learn more about this feature [here](#).
- **Platform Service Account Creation Improvements**: We've enhanced the service user creation workflow, making it easier to set up non-interactive, programmatic access for API integrations and automation scripts. These improvements streamline the process, reducing setup time and complexity. Learn more about this update [here](#).
- **Integrated Windows Authentication (IWA) Host Certificate** (now in GA): In addition to the option to import your own certificate, you can now generate a self-signed certificate with a single click, making setup and management of IWA more efficient. Learn more about this update [here](#).

Engine Management

- **At a Glance view**:
 - Users can view the 'at a glance' summary of the site, including the Engine and its Workloads.
 - Easily check the status of Workloads with fewer clicks.
- **Auto update maintenance window**:
 - Users can choose site-level settings to automatically update their engines.
 - Schedule updates for specific times and days.

Learn more about these updates [here](#).

Marketplace & Integrations

- Download Center (now in GA): Now have ability to download up to 3 previous versions of the software packages. Learn more about this capability [here](#).
- Marketplace Quick Filters - ability to use Quick filters to filter top integrations. Learn more about this update [here](#).
- New and Updated Integrations:
 - Microsoft Defender for Identity Integration with Secret Server (in Private Preview). Learn more about this new integration [here](#).
 - ITP/PCCE: GCP Integration GA
 - MFA: Cisco Duo native in Platform GA
 - Splunk Cloud Integration via Webhooks
 - Direct Entra ID API Integration
 - Workday ITP/CID Integration GA
 - RabbitMQ Helper 12.0.0
 - Terraform SS Integration upgrade 2.0.10
 - Jenkins Release 1.1.0/1.1.1
 - SCIM on prem 4.7.0
 - Secret Server SDK support
 - Terraform 2.0.10
 - ServiceNow Xanadu certification for all Delinea ServiceNow Integrations

Other Updates

- **Webhooks Security** (now in GA): Use webhook secret to verify the legitimacy of the webhook request and protect against man-in-the middle attacks. Learn more about this new feature [here](#).
- **Combined Discovery** (in Public Preview): You can now create and manage both Identity Threat Protection (ITP) and Secret Server (Vault) discovery sources. The two "Sources" pages have been combined under Discovery for a more streamlined experience. Learn more about this update [here](#).

Fall (Q4) 2024 Release

Secret Server (SS) on Platform

- **Entra ID Discovery Expansion**: The discovery capabilities now include the new Entra ID Discovery source and scanners, broadening visibility and access to Entra ID resources. Learn more about this update [here](#).
- **Entra ID Remote Password Enhancements**: A series of updates to improve handling of Entra ID accounts, specifically:
 - Processing heartbeats for Entra ID accounts requiring MFA

Table of Contents

- Processing heartbeats for Entra ID accounts with Conditional Access Policies that enforce MFA.
- Learn more about this update [here](#).

Continuous Identity Discovery (CID)

- **Expanded Identity Coverage:** Improve your organization's identity security with enhanced discovery capabilities in Secret Server Cloud on the Delinea Platform. CID now covers cloud identities including privileged accounts, service accounts, admins, and shadow admins.
- **Automated Monitoring of Sensitive Accounts:** CID operates automatically and continuously, enabling seamless monitoring of sensitive accounts. Privileged credentials can be quickly vaulted in Secret Server as needed, ensuring secure storage and reducing the risk of unauthorized access.
- **Enhanced Discovery and Access Customization:** Easily discover privileged users, including those with stale credentials or lacking MFA. CID also enables quick customization of access, helping you keep user privileges current and aligned with security policies.
- Learn more about this new service [here](#).

Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)

Snowflake Integration:

- **Enhanced User Visibility:** Easily identify and manage user accounts without MFA and partially off-boarded accounts.
- **Privileged Account Discovery:** Detect privileged roles and accounts based on assigned permissions.
- **Comprehensive Health Checks:** Ensure your Snowflake environment's security and compliance with thorough health checks.
- **Attack Detection Rules:** New rules targeting password and MFA-based attacks on Snowflake.
- Learn more about this new integration [here](#).

Privileged Remote Access (PRA)

- **PRA Workloads** (*in private preview*): Unified deployment of PRA capabilities on the Delinea Platform Engine and a centralized Engine Management interface. Learn more about this new capability [here](#).
- **File Transfer Enhancements:** Prevent accidental data loss while transferring files between local and remote systems. Users can see when file transfers are active and they are notified if they try to close the remote connection.
- **Remote Applications:** Access published RDS desktop applications rather than entire systems, enforcing least privilege access and reducing the potential attack surface and associated security risk. Learn more about this new capability [here](#).

Connection Manager (CM)

Available in Connection Manager 2.5.3 Release:

Table of Contents

- **RDP Connection Timeout over TCP:** Connection Manager now allows MacOS users to customize the RDP connection timeout over TCP. This is helpful for extending the timeout in scenarios involving proxy or MFA. Learn more about this update [here](#).
- **MacOS 15 Sequoia Support:** Supports the latest MacOS release.
- **Additional Updates:** More updates and enhancements are detailed in these [release notes](#).

Privilege Control for Servers (PCS)

- **Granular Commands Capability** (*in private preview*):
 - **Minimize Standing Privilege:** Define specific commands within PCS policies for Windows, Linux, and Unix, ensuring users can elevate only what they need.
 - **Enforce Least Privilege:** Limit elevated user actions to pre-approved commands, reducing security risks.
 - **Enhanced Security and Control:** Prevent unauthorized elevated actions with command-level restrictions.
 - Learn more about these new capabilities [here](#).
- **Targeting Machines in AD without Agents:**
 - **Enhanced Policy Targeting:** Apply PCS policies to Active Directory (AD) machines without requiring an agent to be installed first.
 - **Faster Onboarding:** The onboarding process has been streamlined to accelerate time-to-value.
- **Collections** (*in private preview*):
 - **Dynamic Asset Grouping:** Group computers by shared attributes for simplified management.
 - **Streamlined Policy Targeting:** Apply policies to collections, reducing manual effort.
 - **Scalability:** Collections automatically update as new computers meet the defined criteria.
 - Learn more about these new capabilities [here](#).

Identity and Federation

- **Enhanced Security with Duo Integration** (*in public preview*): Customers can enable Duo MFA for an extra layer of security during login and authentication, strengthening their security posture while ensuring a seamless user experience. Learn more about this new capability [here](#).
- **Improved User Experience with Extended Idle Timeout:** The maximum user idle timeout has been increased from 60 minutes to 12 hours.
- **Quick Account Unlock Option:** When users are locked out, Admins can now swiftly restore access to user accounts on the Delinea Platform.
- **New Documented Identity Providers for Federation:** Support has been added for Google, BlokSec, RSA ID Plus, and Celestix.
- Learn more about these new capabilities [here](#).

Platform Engine Management

- **Nomenclature Updates:** Consolidated naming across Engine Management and Platform Engine, including updates to UI, Engine installer, and documentation. Some of these changes will be seen iteratively over the coming months.
- **Improved Logging:** View all Platform Engine and workload logs directly in the Engine Management UI, enhancing supportability.
- Learn more about these new updates [here](#).

Integrations and Marketplace

- **Download Center** (*in public preview*): A dedicated space within the Delinea Marketplace. This new feature simplifies access to a wide range of downloadable resources, including agent updates and tools. Learn more about this new capability [here](#).
- **New and Updated Integrations:**
 - External Secrets Operator with Secret Server
 - MS Sentinel AMA Integrations with Secret Server CEF and Syslog
 - RabbitMQ Helper upgraded to have UI-guided install
 - Jenkins Release 1.0.9
 - Terraform Secret Server Integration upgrade 2.0.8
 - JDBC Proxy for Tomcat and WebSphere upgrade v3.3
 - MidServer Credential Resolver 4.5.2
 - Learn more about new integrations [here](#).

New Authenticator Mobile App

- **New Authenticator Mobile App** (*now in GA*): Introducing a dedicated mobile app for authentication. The app is now available in iOS and Google Play stores.
 - **QR Code Registration:** Users can scan a QR code to register.
 - **Push Notifications:** Receive authentication request notifications on your registered mobile device
 - **Renamed "Authenticator" Tab to "Passcodes"** in the Delinea Mobile application
 - **New Registration Workflow:** Implemented for all mobile applications on the Delinea Platform
 - **Now listed in the Platform Marketplace**
 - Learn more about this new application [here](#).

Other updates

- **Platform APIs** (*now published*): The Platform APIs provide developers with comprehensive access to key platform functionalities. The APIs allow seamless integration, automation, and customization to enhance your Delinea experience:

Table of Contents

- [Platform API Documentation](#)
- [Sample PostMan Collection](#)
- Sample scripts ([PowerShell](#) and [Python](#)) to manage OAuth tokens and test API connectivity for the Delinea Platform. These are simplified examples and might need to be adapted to fit your specific requirements.
- **Platform Service Account:** When you create a service account on the platform, an application account in Secret Server Cloud will now be created automatically, without the need to log in with the service account iteratively.
- **Delinea Expert** (*in public preview*): Delinea Expert is a secure, conversational AI designed to understand and generate human-like text using curated Delinea knowledge. Users can ask questions about platform features, components, or best practices and receive answers with supporting links. Learn more about this new capability [here](#).
- **Webhooks** (*in public preview*): Supports sending platform audit logs to an HTTP webhook endpoint with enhanced event filtering, new webhook logs for better visibility and troubleshooting, and an updated UI for a streamlined experience. Learn more about this new capability [here](#).
- **Tenant IP Restriction:** This new feature enhances the security of your tenant by ensuring that only trusted IP addresses can connect, helping to protect sensitive data and operations. Customers can submit a Delinea support case with their desired IP ranges to apply to their platform tenant.
- **Web Password Filler (WPF):** Support for Manifest v3 as of version 3.10. Learn more about this update [here](#).
- **Enhanced Filtering Experience:** Updated filtering across all platform tables. This feature can be activated using the new user opt-in option under the user's profile preferences, or directly via the tables.
- **Expanded Favorites Functionality:** The *recents* and *favorites* table on the homepage now covers a wider range of objects on the platform, such as pages, secrets, and computers.

Summer (Q3) 2024 Release

Secret Server on Platform

Entra ID Password Changing

- **Alternative to Azure AD PowerShell Modules:** Introduced support for Microsoft Graph API to replace the retired Azure AD PowerShell modules.
- **MFA-Enabled Entra ID Account Passwords:** Added functionality to change passwords for Entra ID accounts with MFA enabled.
- **New Secret Templates:**
 - **Entra ID Application Registration:** Allows for containing and mapping an Entra Application as a privileged account for password changing, using the new OAuth Application Registration extended mapping.
 - **Entra ID User Account:** Enables password changing for an Entra ID account, even with MFA enabled, using the Application Registration.

Remote Access Service (RAS)

- **Rebranding:** Remote Access Service (RAS) has been rebranded to Privileged Remote Access (PRA).
- **Dark/Light Mode Themes:** Now supports dark and light mode color themes, matching the preferences applied to the platform.
- **RemoteApp Assets (Private Preview):** Introduced desktop applications as a first-class inventory object for providing just enough access.
- **File Transfer Usability improvements:** Multiple file uploads and downloads and background file transfers to ensure users can continue to work uninterrupted remotely.
- **Accessibility support:** All PRA menu operations can be accomplished using keyboard controls.
- **Clipboard masking:** Copy confidential information into the PRA clipboard minimizing exposure of sensitive data.

Connection Manager (CM)

Available in Connection Manager 2.5.2 Release

- **Vault Auto-Reauthentication Configuration:** Users can now configure the vault reauthentication behavior. Options include maintaining the existing behavior that automatically restarts the authentication flow or forcing a fresh login when vault session/refresh tokens expire. This feature is especially beneficial for users with longer session/refresh lengths configured through an external identity provider.
- **Machine Field Display:** Connection Manager now displays a "Machine" field from Secret Server, helping users identify the correct target when the secret name is not self-explicit. This field will show in both the Secret Server and Connection Manager grid views.
- **Session Status Popup:** The Session Status popup window, which appeared every time a user signed out of a vault, is now disabled by default. Users can re-enable this pop-up if they encounter memory leak issues.
- **Memory Leak Resolutions:** Addressed various memory leaks to improve performance.

Identity & Federation

- **MFA for Federated Users (now GA):** Federated users can now be challenged for additional MFA within the Platform, including Platform user logon and browser-based step-up MFA such as secret access.
- **Identity Policies Administration:** Significant UX improvements for creating and managing identity policies, including better handling of default values and the flexibility to apply policies globally or to specific groups.
- **Bulk Invite Users:** Administrators can now invite users in bulk from various identity directories, including Delinea and Active Directory (AD). This feature covers AD users who have not yet logged into the platform.
- **New Connector v6.1.350:** Improved the Delinea Connector with a job to refresh "EnvironmentInfo", periodic updates for AD Topology, adjusted refresh intervals based on user changes, and a fix for AD master node syncing issues. Note: Upgrade to v6.1.350 or later by August 31, 2024, to avoid downtime due to major API changes.
- **New Documented Identity Providers for Federation:** Added support for AD FS, Entrust, and OneLogin.

Audit

- **Audit Logging:** Audit logging now supports audit events from various services including Identity, Inventory, and Tenant Profile (tenant customization).
- **Deep Linking:** Added support for deep linking within audit events to easily access users and session recordings.
- **Session Recording Comments** (Private Preview only): Users can now add and reply to comments on each session recording and flag risks.
- **AI-Driven Audit (Private Preview):** Improved AI-driven audit with streamlined call-to-action to run the analysis and a progress indicator.

Permissions

- **Consistency Across Platform Services:** Improved consistency for a more intuitive user interface by leveraging the same Add Member component as Identity.
- **Case Insensitivity:** Users can now search for permissions regardless of case sensitivity.
- **Enhanced Error Messages:** Improved error messages to assist with better troubleshooting.
- **Service Resiliency:** Enhanced resiliency to ensure more reliable performance.

Engine Management

- **Engine State Monitoring:** The engine state is marked as *Unknown* if the engine management does not receive a heartbeat within a specified time.
- **Uninstall Process:** The uninstall process now correctly displays the engine version.
- **Deleting an Engine:** Deleting an engine now clears all associated folders and removes old heartbeats.
- **Default Settings for Workloads** added.
- **All engine pool logs (including workload logs) now stored in:** C:\ProgramData\Delinea Engine\log.

Marketplace & Integrations

- **New Certification Badge, *Delinea Trusted*:** Indicates an integration maintained by a third-party vendor. While Delinea confirms its compatibility, ongoing support should be sought from the vendor's documentation or support channels.
- **Integration Configuration:** Simplified launch into configuring native integrations with a *Configure* button directly from the integrations themselves. This feature is utilized by various integrations, including identity providers for setting up federation providers, among others.
- **ITP/PCCE Integrations:** Introduced new integrations pertaining to Identity Threat Protection and Privilege Control for Cloud Entitlements.
- **New and Updated Integrations:**
 - All ServiceNow integrations certified for the Washington DC release.
 - MID Server Release 4.5.1

Table of Contents

- JDBC Proxy Driver 3.1/3.2 updated to utilize a new encryption method using hardware details to encrypt credentials.
- Rapid7 Insight VM RPC can now be used as RPC with added scripts available in the delineaxpm GitHub repo.
- SCIM Release 4.5.1 for Secret Server only
- RabbitMQ Helper 10.5.0
- Okta and ServiceNow OOB RPC in Secret Server
- MS Sentinel AMA Connector Release for Secret Server
- **Security Upgrades:** Upgraded several packages to resolve security vulnerabilities, including:
 - SCIM Release 4.5.1
 - Terraform 2.0.6

New Authenticator mobile app

- **New Authenticator Mobile App (Private Preview):** Introducing a dedicated mobile app for authentication.
- **QR Code Registration:** Users can scan a QR code to register.
- **Push Notifications:** Easy-to-use push notifications.
- **Authenticator Tab Renamed to *Passcodes*:** The passcode function remains unchanged.
- **New Registration Workflow:** Implemented for all mobile applications on the Platform.

Other updates

- **Updated User Profile:** Enhanced user profile management to include account, security, and application preferences in one place, offering an improved user experience.
- **Global Platform Search (GA):** The global platform search feature is now generally available.

Spring (Q2) 2024 Release

Secret Server on Platform

QuantumLock: Quantum Safe Kyber encryption to secrets

- Prepare sensitive secrets for the growing risk of Quantum Computing.
- Defend against "Harvest Now - Decrypt Later" attacks.

Privileged Remote Access (PRA)

- Background multi-file uploads: Queue files for upload, continue remote work while files transfer in background automatically.
- File Transfers to RDP targets.

Table of Contents

- Support for SMB (v2 & v3) with Windows targets.
- If both SFTP and SMB services are available on the target, PRA will use SFTP (more secure overall). If only SMB is available, PRA will automatically use it instead.
- Keyboard layout support: Easily switch keyboard layouts to match the keyboard layouts configured on target machines.
- Session Connector
 - Configure essential applications for PRA users and limit access to only what's needed
 - Inject Secret Server credentials into running applications
- Connection Info: Access to connection information (such as engine in use, target machine, etc.) for easy identification and troubleshooting when needed.
- Accessibility Improvements: Keyboard can activate and operate PRA menu during remote connections.
- Masked Clipboard for Sensitive Content: Mask sensitive content when using clipboard for data exchange.

Connection Manager (CM)

External Browser Authentication enables users to authenticate to the Delinea Platform through an external browser. This feature facilitates the reuse of existing log-ins, password managers, and advanced functionalities such as biometric MFA, FIDO2 support, and conditional access configurations with their chosen identity provider.

Inventory

Inventory is now generally available, offering users a new interface to view and remotely connect to target machines, utilizing:

- My Account: Users can log in to enrolled Linux systems with their Delinea Platform account, either via the platform or through native applications using SSH, SCP, or SFTP.
- Vaulted Credentials: Users can access any target system in the Delinea Platform using vaulted credentials from Secret Server.
- Manually Entered Credentials: Users can manually log in to target systems with valid username and password.

Audit

- Audit Logging is now generally available, supporting audit events from various services:
 - Secret Server
 - Privileged Remote Access
 - Permission Service
 - Audit Collector (included in Privilege Control for Servers)
 - Policy Service
 - Federation Service
- Sharing of recordings: Share links to recordings (with specific timestamps) with other users on the platform.
- Terminate Live Remote Sessions: Available for Privileged Remote Access and Secret Server.

Marketplace & Integrations

- Launch of the Delinea.com [Integrations Center](#)
- Addition of Community-provided integrations: These are scripts developed by external contributors and hosted on [Delinea's GitHub repository](#). They are not officially maintained by our development team and are provided "as is" with no guarantees on performance or compatibility.
- New and updated integrations:
 - SNOW MID Server 4.5
 - JDBC Proxy Driver 3.0
 - Rapid7 Insight VM Integration with Secret Server for Shared credential Sync
 - SCIM Release 4.4.4
 - Terraform 2.0.4/2.0.5
 - UiPath 2.6.0
- New Download Center (currently limited to Privilege Control for Servers customers)
- Enhanced user experience:
 - Updates to certification and vendor filters
 - Improved support for light and dark mode
- Significantly increased the number of integrated vendors.

Identity & Federation

- Add bulk users to the local directory: This feature allows administrators to import a large number of user accounts simultaneously, streamlining the process instead of adding users manually to the Delinea Directory one by one.
- MFA for federated users (private preview): Federated users can be challenged for additional MFA within the platform: This includes platform user log on and any browser-based step-up MFA, such as secret access.
- Ability to map a large number (beyond the previous limit of 100) of identity provider groups to platform groups.

Platform Engine Management

- Platform Engine Management is now available for general use.
- Support for two Privilege Control for Server (PCS) workloads: Command Relay and Audit Collector.
- Engine auto-upgrade to new versions and remote uninstallation are now supported.
- Utilize vaulted accounts within workload management settings.

Privilege Control for Servers

Introduction of the 'Require Session Recording' rule to manage recording during endpoint login and privilege elevation via policy, ensuring that login or elevation is prevented if host-based recording is cannot be initiated.

Delinea Mobile App

In Delinea Mobile 2.3 release, Offline Caching was introduced, aligning with the existing feature in our Secret Server Mobile app. This release offers:

- Single Secret downloads
- Consolidated offline view
- Expiration indicator
- New “Download” filter
- Download indicators per secret

Web Password Filler (WPF)

TOTP support was introduced in 3.9 release. With this update, you can generate and copy TOTP codes directly from the WPF browser extension. The code length is adjustable by the admin and operates on a 30-second loop.

Other updates

- New navigation interface offers a use-case-centric view of our platform services, with content categorized to reflect service relationships. This enhanced experience offers:
 - Simplified navigation for common use cases.
 - Ability to access available pages without redirection.
 - Customizability with expanded/collapsed views.
 - Swift access to frequently used features.
- The global platform search (private preview) has been updated to deliver more results, encompassing Assets & Marketplace outcomes, along with content. Content searches now include page titles and descriptions, enabling streamlined access to most products from a single search query.
 - Access all items from a single-entry point, minimizing menu navigation.
 - Uncover pertinent configurations based on keyword searches.
- Improved uptime SLA for platform now 99.99%. More information can be found on <https://delinea.com/sla>
- New Trust Center - <https://trust.delinea.com/>
 - Get Trust Center Updates in your inbox.
 - Access compliance documents such as ISO 27001 and SOC2 reports.
 - Stay informed about published vulnerabilities and their fixes.
 - Submit and report vulnerabilities.

Winter (Q1) 2024 Release

Secret Server on Platform

- Ongoing UI conversion to the same modern development framework as the rest of the product (Angular), covering Launcher configuration, dependency configuration, Remote Password Changer, and Heartbeat configuration screens.
- Discovery now retrieves zone metadata and additional Active Directory attributes, enabling identification of discovered AD assets with Privilege Control for Servers data, export to, and matching within the Inventory service.

Privileged Remote Access (PRA)

- File transfer to and from SSH targets
- PRA engine host sizing guide
- PRA engine host hardening guide
- Private Preview - RemoteApp support
- Readiness for Privilege Control for Servers

Connection Manager (CM)

- Supports MacOS Sonoma
- Supports Privilege Control for Servers (PCS) MFA-on-endpoint for AD-Joined SSH targets
- Check out a secret for exclusive access and extend time from within CM

Audit

- Combine Secret Server sessions alongside Platform sessions
- User experience enhancement throughout for better usability, including deep linking to other resources.
- Improvements to the quality and performance of transcription and anomaly detection - now available in Private Preview.

Marketplace & Integrations

- Integrations expanded to include multiple new listings for federation to IDPs, with various updates to existing integrations like PowerShell and Terraform.
- By default, Marketplace View Permissions are accessible exclusively to admin users.

Identity & Federation

- The Federation underwent a comprehensive UX/UI redesign, simplifying the Identity Provider creation process by eliminating wizards, enhancing automation to minimize configuration overhead, and introducing clearer visual cues for mandatory user mappings.

Table of Contents

- Connector version 5.1.8 has been released with enhancements focused on improving reliability, stability, and extensibility. While earlier Connector versions will continue to function without service disruption, registration or re-registration of these versions with the Platform after Feb 15, 2024, may not successfully complete. It is advisable to upgrade your Connector to version 5.1.8 or the latest before the specified date.
- The Authentication Profiles settings page has undergone a complete UX/UI overhaul, introducing a new "Description" field and eliminating pop-up screens for configuring settings.

Other updates

- "Use my Account" is now available as a launch option (only for Linux machines)
- New Platform tenants will experience "Unified Mode" for Roles and Permissions - one management plane for all permissions.
- Customers now have the option to participate in the Public Preview program, allowing them to personally explore, test, and offer feedback on new enhancements before the official General Availability (GA) release.

Fall (Q4) 2023 Release

Secret Server on Platform

- The General Availability (GA) of Step-up Multi-factor Authentication (MFA) for Secrets is now available.

Privileged Remote Access (PRA)

- Introducing enhanced control for PRA clipboard functionality access
- Improved troubleshooting with more specific and detailed error messages
- RemoteApp support has entered Private Preview, allowing isolation of remote access to individual applications, rather than the entire desktop.

Web Password Filler (WPF)

- Early Access is now available for WPF 3.7, featuring support for synchronizing recent and favorite secrets in Secrets.
- You can now search for any web secret directly from the Recent tab.

Connection Manager (CM)

- Support for step-up MFA for Secrets

Integrations and Marketplace

- Introducing global search capability within the platform
- Various improvements to content and layout
- New permissions have been added, including download and view permissions.
- Integration updates:

Table of Contents

- RabbitMQ: Now supports several new commands and the latest stable versions of Erlang and RabbitMQ
- JDBC Proxy Driver: Offers support for multiple data sources and enhanced credential validation for WebSphere and Tomcat.
- Ansible - RedHat Ansible Secret Server collection Certification
- SCIM on premise: Upgrades include enhanced logging, role assignment additions, and updates to the configuration page.
- UiPATH Orchestration on premise: Enhanced token expiration support for API calls, enabled retry functionality by default, and improved credential encryption.
- SDK plugins - Addressed all Open vulnerabilities
- ServiceNow: Upgraded ServiceNow MID Server Integrations, added support for SNMPv3 Credentials, and credential encryption utility.

Identity & Federation

- We now provide platform federation support for SAML and OIDC with Ping Identity (PingOne).
- IDP-initiated Single Sign-On (SSO) flow is now supported.
- Introducing the Federation Debug Console, a self-service debugging tool for troubleshooting federation setups with Identity Providers (IdPs).
- Third-Party MFA Servers (via Radius) now Generally Available (GA).
- We have introduced a set of documentation and example scripts on GitHub to automate the installation of the Delinea Connector.
- Introducing a new set of federation settings:
 - Customize Issuer Sent To IDP: This setting allows you to override the default Certificate Issuer (Entity ID) sent to the Identity Provider (IdP).
 - Request Binding: This setting controls the method for binding SAML authentication requests to the communication protocol.
 - Sign Request: This setting ensures that SAML authentication requests sent to the IdP are digitally signed for enhanced security.
- You can now verify the status of the Delinea Connector using the new Ping Connector capability.

Other updates

- Introducing new UX updates to the platform's user profile.
- Asset View is now available in Private Preview, offering users a new way to access inventory by machine and enabling remote session invocation.
- Improved roles and permissions: The Everybody group can now be removed from the Platform User role, providing greater permission customization.

Summer (Q3) 2023 Release

Secret Server on Platform

- MFA (Mufti Factor Authentication) on Secret access, now in Private Preview, is a new security mechanism designed to enhance the protection of sensitive credentials and privileged information stored within Secret Server's vault. MFA on Secret access helps ensure that only authorized individuals with the correct authentication factors can retrieve these valuable credentials.
- Improvements to Discovery UI and overall user experience

Privileged Remote Access (PRA)

- Additional logging and diagnosability to effectively identify and resolve issues
- Support for HTTPS PROXY by the PRA engine
- Support for remote access to target systems using Secret Server RDP proxy configurations

Web Password Filler (WPF)

- Web Password Filler v3.5.3: Users can now log in to their Delinea Platform tenant from WPF.

Connection Manager (CM)

- Connection Manager v2.0: Users can now log in to their Delinea Platform tenant from CM.

Audit

- Simplified, intuitive navigation for session recordings
- Enhanced playback controls: full screen and zoom features are now supported
- Improved responsiveness to live streaming and encoding processes
- Secret name now included and deep linked on the session recordings

Marketplace & Integrations

- This update brings a complete overhaul of the user experience for Marketplace:
 - Consolidated tabs for Applications and Tools and Integrations tabs
 - Both tabs now have dynamic filters relative to each tab which simplifies searching for specific or available integrations.
 - Marketplace cards have been updated to clearly identify Vendor, Integration name, supported Application, and certifications, for faster search.
 - Details pages have been redesigned to have more descriptive content.
 - Details pages no longer show full documentation, and instead link to the appropriate documentation articles.
- Integrations added or updated for Secret Server on the platform:

Table of Contents

- Palo Alto XSOAR v3.0.1: Introduces a new capability to allow users to add automated comments which will display under Secret Server Audit.
- PowerShell Module v0.61.3: Updated the package to resolve the cryptography vulnerability and updated SS (Secret Server) SDK to v1.5.3.
- UiPath v2.2.0: Resolved issues with multiple SDK accounts being created on a Secret Server. SDK account details are now stored in the config file (in encrypted format) in the user temporary directory.
- Ansible plugin: updated to allow secrets calls by path and ID.
- SCIM for Secret Server, Multiple Releases (Current v4.4.1): Streamlined integration with IGA providers, and resolved vulnerability issues.
- RabbitMQ Helper, Multiple Releases (Current v10.2.0): addressed reported issues, and added the ability to upgrade RabbitMQ using a URL provided by the user.

Identity & Federation

- Simpler workflow for adding local users: This enhancement aims to streamline the process of creating new local users in the platform, by reducing the steps it takes, making it easier and more efficient for administrators.
- Visibility in users' platform login activities: log of all recent login activities associated with a user's account. This includes information such as date, time, source IP address, browser, and OS details of each login attempt.
- Third Party MFA Servers (via Radius), now in Private Preview. You can use your RADIUS server to authenticate users to the Delinea Platform. RADIUS authentication can be used with Multi-Factor Authentication (MFA) to provide an additional security layer.
- Delinea Connector auto-update support: you no longer need to manually download and install Delinea Connector updates. The platform can now automatically handle the update process in the background, ensuring that you always have the latest version of the connector without any effort on your part.
- Streamlined the user experience flow to download the Delinea Connector and generate its registration code.
- Force Re-authentication with Identity Providers (IdP): By default, federated users are not prompted to re-authenticate with IdPs every time they try to log on to the platform, assuming the user has a valid authentication session with the IdP. The introduction of this capability in platform helps where this experience may not be desired, such as on shared workstations and/or if re-authentication is required where sensitive operations are performed with requirements for governance and assurance.

Other updates

- Global Search: powerful search functionality empowers you to find everything you need across the platform. This capability is now limited to search across Secrets, with plans for further integration across the entire platform.
- Ability to dismiss the platform set up flow: you can now choose to skip the onboarding setup tasks, tailoring the onboarding process to your specific needs.

Spring (Q2) 2023 Release

New Hosting Regions

The Delinea Platform is now available globally in the following geos

- US
- Canada
- Europe
- Australia
- UK
- Southeast Asia

Behavioral Analytics (Private Preview)

Now in Private Preview, Behavioral Analytics is the next evolution of our standalone Privileged Behavioral Analytics, seamlessly integrated with everything on the Delinea Platform to showcase the power of a unified cloud-native platform. Highlights:

- ML-powered anomaly detection
- A user-friendly interface that makes it easy to get started with Behavioral Analytics
- Powerful data-visualization that helps to quickly identify anomalous patterns and potential risks

Contact your Sales rep if you'd like to try it before GA.

Permissions Service

- This new service helps platform administrators define roles and assign specific permissions to each role.
- Users or groups can then be assigned to these roles, thus inheriting the expected defined privileges.
- This service allows for a flexible and scalable way to manage access controls and ensures that only authorized users have access to sensitive resources.
- Supports both custom and built-in roles
- Offers fine-grained controls over access to resources
- Simplified UX to manage roles and permissions

Improved Home Screen

- Complete UI overhaul of the platform home screen
- Added a new platform onboarding task list

Marketplace

- The New Delinea Marketplace is your one-stop shop for Delinea applications, partner integrations, and direct downloads.

Table of Contents

- Dynamic Category Search Drop-Down is now available
- Many new integrations added, including Microsoft Sentinel and ConnectWise Control
- Mobile App has been added

Tenant Customization

Customers can now update the look and feel of the platform tenant portal to suit their corporate branding.

Features:

- Add custom terms/privacy notices
- Add company name
- Add corporate logo (dark/light mode support)
- Set banner
- Username format/display hint

Winter (Q1) 2023 Release

Seamless Integration with Secret Server Cloud

Existing Secret Server Cloud users can view and manage secrets entirely within the Delinea Platform with a familiar user experience. Users can fully leverage the platform as their primary interface for their day-to-day use of Secrets

Next-Gen Privileged Remote Access

- Launch secure VPN-less browser-based SSH and RDP sessions with a single click
- Agentless deployment – no additional software is required on target hosts
- No end-user clients required – based on a modern HTML5-based web client
- Zero impact on customer security posture – no inbound firewall rules to open
- Agentless session recording to meet customers' audit and compliance requirements

Robust Identity and Federation Services

- Support for Active Directory
- OIDC Federation, SAML support
- Policy-based MFA (including FIDO2, Passkey, etc.) for platform login

Marketplace

The New Delinea Marketplace is your one-stop shop for Delinea applications, partner integrations, and direct downloads.

Foundational Shared Services

A wide range of unified services such as authentication, notification, and federation services.

Preview Program

Delinea offers two programs for previewing features in development: Private Preview and Public Preview, described below. Typically, features graduate from Private Preview to Public Preview status, although a feature could in some cases go directly from Private Preview to General Availability (GA).

To submit feedback, use the feedback button near the top right corner of every Delinea Platform page. The feedback you provide during the preview period is crucial input for further feature refinement and enhancing overall usability.

Public Preview

You can now choose to opt in to the Public Preview program on your own, to experience and explore new platform enhancements and provide feedback before their official General Availability (GA) release.

You cannot opt into or out of individual Public Preview features. When you opt in, you opt in to all Public Preview features, and when you opt out, you opt out of all Public Preview features. Public Preview features appear on the customer documentation portal as any GA feature would but with a notation at the top specifying that the feature is available only as a Public Preview.

Opt In

By default, you are not opted in. To participate in the Public Preview program, follow these steps:

Prerequisite: Required permissions: `delinea.platform/administration/tenantprofile/update`

1. From the left navigation, select **Settings**, then select **Tenant customization**.
2. Click **Preview Preferences**.
3. Review the information and disclosures about the Public Preview program.
4. Select the Opt-in checkbox in the bottom left corner.
5. Click **Save**.



Note: It may take up to five minutes for these preview features to become visible and accessible in your Delinea Platform tenant.

Opt Out

You can choose to stop participating in the public preview at any time by simply de-selecting the Opt-in checkbox described in "Opt In" above.



Note: It may take up to five minutes to deactivate any public preview feature in your Delinea Platform tenant.

Current Public Preview Features

The features currently available in Public Preview are listed in the following table. This list is subject to frequent updates.

Table of Contents

Feature	Description	Documentation
AD Rapid Discovery	AD Rapid Discovery maintains continuous synchronization between Active Directory (AD) and the Delinea Platform.	"AD Rapid Discovery Workload" on page 267
Combined Discovery	Delinea ITP/PCCE customers can view both Secret Server (Vault) and Threat Protection (ITP) sources, run scans, and select which type of source to create from a single place. Users with only vault will be able to preview what ITP sources are available with links directly to Marketplace.	Combined Discovery
Favorites and Recents	You can mark all platform configuration pages and most details pages as Favorites by selecting the star icon at the top of the page. You can then access your favorited pages at Home > Favorites. You can also access your recently-visited pages, at Home > Recents.	Favorites and Recents
Analytics	Analytics on the platform empowers IT and security administrators to prevent, detect, and stop breaches by continually monitoring alerts across the organization to identify early signs of threats.	"Analytics" on page 161
AIDA	AIDA (AI-Driven Audit) automatically reviews privileged SSH and RDP recordings with computer vision and large language model (LLM) analytics. It turns hours of video into a searchable audit trail, pinpointing elevated commands and risky behavior so PAM, security and audit teams can find answers in seconds.	Analyzing a Recording with AIDA
Standalone PRA Engine Upgrade to the Delinea Platform Engine	Upgrade your deprecated standalone PRA Engines to Platform Engine Management and PRA capabilities with a single click.	"Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

Private Preview

Delinea invites a small set of specific customers to preview upcoming features and capabilities of the Delinea platform. Private Preview features are not covered by Support services or by any SLA. Private Preview features appear on the customer documentation portal as any GA feature would, but with a notation at the top specifying that the feature is available only to customers participating in the private preview of that feature.

Current Private Preview Features

The features currently available in Private Preview are listed in the following table. This list is subject to frequent updates.

Feature	Description	Documentation
Engine Management: Using the AD Rapid Discovery Workload	AD Rapid Discovery maintains continuous synchronization between Active Directory (AD) and the Delinea Platform. The Windows Server Manager can be used to change computer properties within AD. Any changes made to computers in AD trigger real-time synchronization through AD Rapid Discovery to the Server Suite Agent, and the changes appear on the Delinea Platform. Changes to the computer where AD Rapid Discovery is running appear in the Inventory page of the platform after synchronization.	Engine Management: AD Rapid Discovery Workload
Identity Lifecycle Management	Each organization's systems and identities are unique and there is no single setup process that must be followed for optimal configuration. ILM is part of Identity Governance Administration (IGA).	ILM: Setup and Configuration
Platform Integration Center	This feature is for customers already using Secret Server Cloud who wish to migrate to Secret Server on Platform. When you use the Platform Integration Center to integrate Secret Server and the Delinea Platform, the platform and Secret Server run with unified administration. Management of roles and permissions transfers completely to the platform, and they become read only in Secret Server.	Platform Integration Center

Platform Architecture

Click the link to view the [Platform Architecture](#) diagrams.

Customer Firewall Requirements

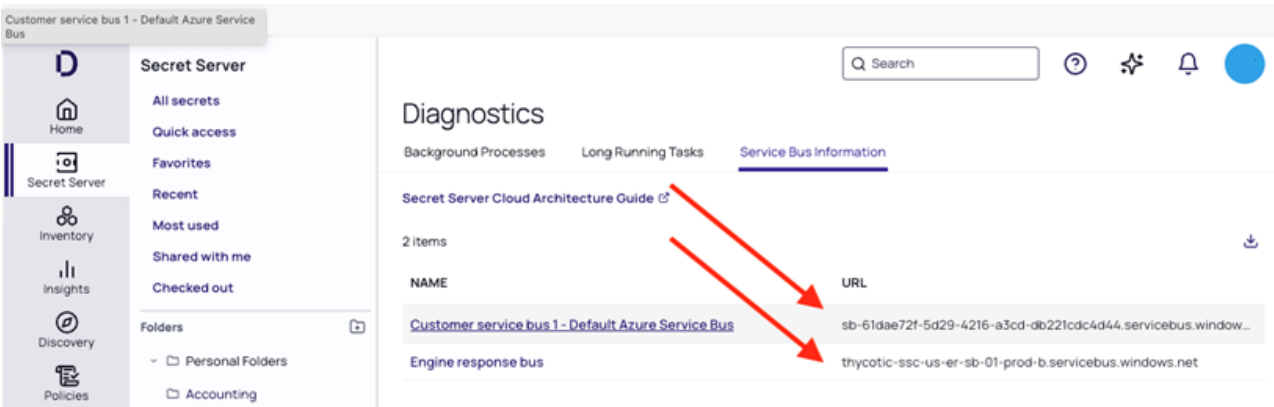
If your environment has a firewall, you must provide access from your corporate environment out to the Delinea Platform.

Key Terms:

- *PCS* is the Privilege Control for Servers feature of the Delinea Platform.
- *PRA* is the Privileged Remote Access feature of the Delinea Platform.


Determining Your Tenant's Customer Service Bus and Engine Response Bus

1. Go to the URL for your platform tenant: <https://<tenant>.delinea.app/view/vault/diagnostics/system/service-bus>
2. Locate the Customer Service Bus and Engine Response Bus Information shown in the diagram.
These URLs are generated during the setup of Platform.



3. Ensure that both of the FQDNs are given outbound https access.

U.S. Tenants

 **Note:** These firewall rules must be configured with SSL Inspection *disabled*. The services will not function if they detect an intermediate certificate for SSL inspection

URLs (SSL 443 Outbound)	Notes
<tenant>.delinea.app <tenant>.secretservercloud.com downloads.marketplace.delinea.com	URL for the platform tenant. URL for the Secret Server tenant Access to the Marketplace site for software downloads

Table of Contents

URLs (SSL 443 Outbound)	Notes
prod-tcpr-1.eastus.cloudapp.azure.com prod-tcpr-2.eastus.cloudapp.azure.com prod-tcpr-3.eastus.cloudapp.azure.com prod-tcpr-4.eastus.cloudapp.azure.com prod-tcpr-1.westus.cloudapp.azure.com prod-tcpr-2.westus.cloudapp.azure.com prod-tcpr-3.westus.cloudapp.azure.com prod-tcpr-4.westus.cloudapp.azure.com	TCP Relays are VMs using custom code.
enginepoolupdateprod.blob.core.windows.net authstorprod8138094.blob.core.windows.net enginepool-downloads-prod.azureedge.net	Microsoft .NET services for the Engine Pool. CDN for the Download center.
bobbish-coral-anteater.rmq4.cloudamqp.com dramatic-coral-crow.rmq2.cloudamqp.com fast-green-crab.rmq2.cloudamqp.com loud-beige-duckbill.rmq5.cloudamqp.com	RabbitMQ for Engine Management
*.lencr.org (http) *.digicert.org (http)	Certificate Validation URLs (port 80 http traffic only) Connector requires digital certificate validation at letsencrypt.org and digicert.
Engine Response Bus (FQDN) Customer Service Bus (FQDN)	Enter these URLs from your platform tenant. They are generated during platform setup.

Non-US Tenants

URLs (SSL 443 Outbound)	Notes
<tenant>.delinea.app <tenant>.secretservercloud.com downloads.marketplace.delinea.com	URL for the platform tenant URL for the Secret Server tenant Access to the Marketplace site for software downloads
enginepoolupdateprod.blob.core.windows.net authstorprod8138094.blob.core.windows.net enginepool-downloads-prod.azureedge.net	Microsoft .NET services for the Engine Pool. CDN for the Download center.

Table of Contents


URLs (SSL 443 Outbound)	Notes
*.lencr.org (http) *.digicert.org (http)	Certificate Validation URLs (port 80 http traffic only) Connector requires digital certificate validation at letsencrypt.org and digicert.
Australia	prod-tcpr-1.australiaeast.cloudapp.azure.com prod-tcpr-2.australiaeast.cloudapp.azure.com technical-blond-elk.rmq2.cloudamqp.com (include US Addresses below for backup)
Canada	prod-tcpr-1.canadacentral.cloudapp.azure.com prod-tcpr-2.canadacentral.cloudapp.azure.com smart-orange-gibbon.rmq2.cloudamqp.com (include US Addresses below for backup)
Europe	prod-tcpr-1.westeurope.cloudapp.azure.com prod-tcpr-2.westeurope.cloudapp.azure.com young-azure-hare.rmq2.cloudamqp.com (include US Addresses below for backup)
Southeast Asia	prod-tcpr-1.eastasia.cloudapp.azure.com prod-tcpr-2.eastasia.cloudapp.azure.com hippy-fuchsia-woodpecker.rmq2.cloudamqp.com (include US Addresses below for backup)
United Arab Emirates	prod-tcpr-1.uaenorth.cloudapp.azure.com prod-tcpr-2.uaenorth.cloudapp.azure.com young-olden-buffalo.rmq6.cloudamqp.com (include US Addresses below for backup)
United Kingdom	prod-tcpr-1.uksouth.cloudapp.azure.com prod-tcpr-2.uksouth.cloudapp.azure.com giant-maroon-bullfrog.rmq3.cloudamqp.com (include US Addresses below for backup)

URLs (SSL 443 Outbound)	Notes
United States: Include these backup addresses in your firewall table. Emergency failover is routed to the US regions.	prod-tcpr-1.eastus.cloudapp.azure.com prod-tcpr-2.eastus.cloudapp.azure.com prod-tcpr-3.eastus.cloudapp.azure.com prod-tcpr-4.eastus.cloudapp.azure.com prod-tcpr-1.westus.cloudapp.azure.com prod-tcpr-2.westus.cloudapp.azure.com prod-tcpr-3.westus.cloudapp.azure.com prod-tcpr-4.westus.cloudapp.azure.com
Engine Response Bus (FQDN) Customer Service Bus (FQDN)	Enter these URLs from your platform tenant. They are generated during platform setup.

Inbound Filtering

Customers interested in implementing inbound filtering can restrict access to traffic originating from the Delinea Platform to the specified egress IP address ranges below:

- 4.180.243.168/29
- 13.68.202.64/29
- 20.11.207.32/29
- 20.90.1.200/29
- 23.100.88.32/29
- 23.101.212.8/29
- 40.85.216.32/29
- 40.85.241.48/29
- 40.86.243.40/29
- 51.140.10.160/29
- 51.145.8.56/29
- 65.52.165.168/29
- 74.235.247.24/29
- 104.210.77.120/29
- 104.215.150.80/29
- 108.143.39.32/29
- 137.116.238.240/29
- 172.203.27.16/29

 **Important:** To ensure proper configuration, you must refer to the [Secret Server Hybrid Multi-Tenant Cloud Architecture](#) for detailed information on the required ingress and egress IP ranges used by Secret Server Cloud.

Ports and Network Communication

Port 443 (outbound only) must be open for the engine to send encrypted information to the platform through the message queue service.

Outbound Message Queue - Fully Qualified Domain Names (CloudAMQP)

The following Fully Qualified Domain Names are deployed by CloudAMQP using public IP ranges of Amazon, Azure, DigitalOcean, and Google Cloud, and are used by the engine to facilitate communication with the platform through encrypted messages over the CloudAMQP messaging service.

Outbound firewall rules should include the following Fully Qualified Domain Names (selected by databoundary), rather than static IP ranges of these URLs, as these IP ranges can change.

Australia	technical-blond-elk.rmq2.cloudamqp.com
Canada	smart-orange-gibbon.rmq2.cloudamqp.com
EU	young-azure-hare.rmq2.cloudamqp.com
SEA	hippy-fuchsia-woodpecker.rmq2.cloudamqp.com
UAE	young-olden-buffalo.rmq6.cloudamqp.com
UK	giant-maroon-bullfrog.rmq3.cloudamqp.com
US	dramatic-coral-crow.rmq2.cloudamqp.com loud-beige-duckbill.rmq5.cloudamqp.com fast-green-crab.rmq2.cloudamqp.com bobbish-coral-anteater.rmq4.cloudamqp.com



Notes:

Engines cannot be installed on domain controllers.

When using PowerShell, version 7.3 is recommended for optimal performance. Version 5.1 may result in suboptimal performance.

Engines use the Message Queue service to queue encrypted messages, which are then consumed by Engine Management. Engine Management, in turn, uses Message Queue encrypted messages for engines. These queues are separated by regional data boundary. Messages are encrypted and decrypted by tenant. For successful communication between

Privileged Remote Access

Delinea Privileged Remote Access (PRA) provides seamless access to remote machines through RDP and SSH, without the need for a VPN. PRA leverages a PRA engine that runs on customer premises.

No internet-facing ingress ports are required for the PRA Engine. Only TLS 1.2+ is supported. See [Setting Up a Platform Firewall](#) for internal and external access ports.

Internal Access on these ports

- 22 TCP from PRA Engine to Linux-based target machines for SSH access.
- 53 TCP/UDP from PRA Engine to DNS server for name resolution of target machines.
- 443 TCP from PRA Engine to Secret Server (on-premise) to enable integration with the Delinea Platform and leverage secret access. Only required if Secret Server (on-premise) is in use.
- 445 TCP from PRA Engine to Windows-based target machines for SMB file transfers.
- 3389 TCP from PRA Engine to Windows-based target machines for RDP access.

Outbound Access on port 443 TCP

- from PRA Engine to the Delinea Platform through Message Queue ingress.
- from the Secret Server (on-premise) to the Delinea Platform through Message Queue ingress to support the integration.

Delinea Connector

The Delinea Connector enables secure communication between the Delinea Platform and AD directories. Typically, the Delinea Connector is installed on-premises and requires access to an Active Directory Domain Controller.

- Outbound access required on port 443 TCP from the Connector to the Delinea Platform through WAF.
- No internet-facing ingress ports are required for the Connector.



Note: Requests from the Delinea Platform to the Delinea Connector are made through the TCP Relay hosts. For example, such requests include querying for AD user details. All data is encrypted.

Region	TCP Relay Hosts IP Address Range
Australia	20.211.60.240 - 20.211.60.247
Canada	20.104.14.80 - 20.104.14.87
Europe	20.8.3.112 - 20.8.3.119
Southeast Asia	20.195.89.80 - 20.195.89.87
United Arab Emirates	20.203.77.200 - 20.203.77.207

Table of Contents

Region	TCP Relay Hosts IP Address Range
United Kingdom	20.49.210.72 - 20.49.210.79
United States	20.242.252.136 - 20.242.252.143; 52.148.145.72 - 52.148.145.79; 20.85.110.128 - 20.85.110.135

- The Delinea Connector requires internal access for the following ports:
 - 53 TCP/UDP to DNS server for name resolution (this might be the DC itself depending on your environment)
 - 88 TCP to AD Domain Controller used for Kerberos authentication
 - 123 UDP to AD Domain Controller for time synchronization
 - 135 TCP to AD Domain Controller for remote procedure call (RPC) endpoint mapping
 - 389 TCP/UDP to AD Domain Controller for handling normal authentication queries
 - 3268 TCP to AD Domain Controller for Global Catalog access
 - 9521 TCP from the Delinea Connector Configuration process to the DelineaProxy service for RPC communication.

Privilege Control for Servers (PCS) Agent

The PCS agent requires internal access for the following ports:

- 8443 TCP and 8080 TCP for the Delinea Connector
- 5063 TCP to for the Audit Collector

Notification Services

The platform leverages select third-party messaging providers. This enables Delinea to deliver notifications promptly and reliably to users across various channels, including email, SMS, and phone.

Vendor	IP Address	Purpose (examples)
AWS SES	54.240.75.72 54.240.75.73	The Delinea Platform uses AWS SES as its primary email service provider for a variety of email notifications, including user invitations to the platform and email MFA code pins.
SendGrid	149.72.129.10	SendGrid is the primary email service provider for Secret Server email notifications, particularly for tasks such as access requests.
Twilio	--	Twilio is used for SMS and Phone MFA.

Tenant IP Restrictions

The Tenant IP Restrictions feature ensures that only trusted network IP addresses or CIDR ranges can connect to your Delinea Platform tenant. By limiting access to approved network ranges, this feature adds an extra layer of security to your environment.

Key Benefits

- **Enhanced Security:** Restricts access to only approved IP addresses, reducing the risk of unauthorized access.
- **Comprehensive Coverage:** Applies to both the Delinea Platform tenant and the integrated Secret Server Cloud instance, ensuring consistent protection across the entire environment.

Submitting an IP Restriction Request for the Platform

To enable IP restrictions, submit a support case to Delinea Support with the list of allowed IP addresses or CIDR ranges. Delinea Support will assist in configuring the allowlist for your tenant to ensure seamless and secure access.

When submitting a request, please ensure the following:

- **Maximum Address Limit:** The request must contain no more than 50 individual IP addresses or CIDR blocks combined.
- **No Duplicate Addresses:** The request must not contain any duplicate IP addresses.
- **Exclude Reserved IPs:** Do not include any of the Delinea-owned IP addresses.
- **CIDR Block Standards:** Submitted CIDR blocks must follow strict standards. For example, a /29 block must align with valid start addresses.
 - *Invalid:* 192.0.2.20/29
 - *Valid:* 192.0.2.16/29

Failure to meet these requirements may result in delays or rejection of the request.



Note: Ensure that all necessary IPs are included to avoid unintended access disruptions.

Delinea Expert

Delinea Expert is an AI chatbot. Ask it any question about the Delinea Platform's features, components, or best practices. Delinea Expert provides links to support its answers.

Delinea Expert cannot access your data or see which platform page you are on.



Delinea Expert can sometimes make mistakes. Always check important information. If an answer seems inaccurate, click the Flag icon to alert Delinea. For more information, see [Troubleshooting Delinea Expert](#).

Accessing Delinea Expert

To open a Delinea Expert window:

- Click the sparkle icon in the top bar of the platform interface.

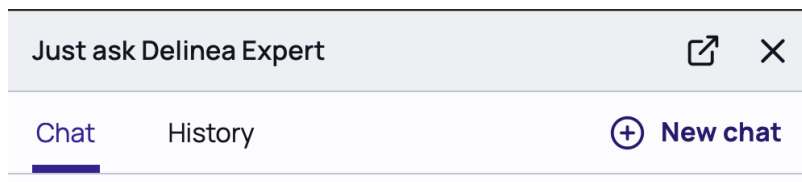


A pane opens to display the Delinea Expert interface.

To close Delinea Expert:

- Click the **X** in the upper right corner.
- Click the sparkle icon in the top bar.

 **Tip:** : You can move Delinea Expert to a separate browser tab by clicking the pop-out icon next to the **X**.



To start a new conversation, click **New chat**. This can help you to start with a clean slate, or to focus your conversations on specific topics.

To view past chats, click **History**.

You can return to your current chat by clicking it in the **History** list or by clicking **Today** (when available).

Interaction Tips

Interaction with Delinea Expert is similar to any modern Large Language Model (LLM):

- Type your question (also known as a “prompt”) in plain language.
- To submit your prompt, either hit the enter key or click the send icon in the lower right of the text entry field.
- The resulting answer includes links to the relevant information sources. We highly recommend reviewing these links to ensure the answer is accurate.

Questions are most effective when they:

- Are focused on a single topic
- Clearly specify a platform feature you want to use
 - For example, Secret Server, Privilege Control for Servers (PCS), Privileged Remote Access (PRA), Identity Threat Protection (ITP), or Privilege Control for Cloud Entitlements (PCCE).

Examples of effective prompts include:

Table of Contents

- How do I set up Privileged Remote Access?
- Where can I find the remote access logs?
- Where do I download the Delinea Platform Engine?
- How do I onboard users from Active Directory?

For troubleshooting common issues, you can ask general questions or include specific error messages like:

- Why can't I connect to the Privileged Remote Access?
- Connector installation failed to obtain certificate. Now what?
- Where do I find the log files for PCS?
- I installed the Delinea Platform Engine but I don't see it in Engine Management.

Delinea Expert can also answer questions about best practices in Privileged Access Management and Identity Security, based on the blogs and white papers on Delinea's website.

Additional Uses

Delinea Expert can do more sophisticated things than summarizing documentation.

- **Translation:** Delinea Expert can answer in any language that OpenAI currently supports. Simply type questions in your preferred language to receive answers in that same language.
- **PowerShell Scripts:** You can request PowerShell scripts for various administrative tasks. For example, "Generate a PowerShell script to list all users in Active Directory."
- **Logs and Reports:** Delinea Expert can guide you on how to interpret logs and reports. Ask questions like, "What does this log entry mean?" or "What is the likely cause of an error based on this HAR file?" Expert will ask you to paste the text and will provide an analysis.

Troubleshooting Delinea Expert

Delinea Expert can sometimes make mistakes – always check important information.

If an answer seems inaccurate, you can resolve it a few ways:

- **Tell Delinea Expert it was wrong:** When you correct Delinea Expert, it helps to tell it why the answer was wrong, and to rephrase the question with more detail. Delinea Expert will use the new information to search.
- **Start a new chat:** If previous questions and answers are about unrelated topics, sometimes starting a new conversation (by clicking **New chat** in the upper right) can help by clearing that content from memory.
- **Flag the answer:** Click the Flag icon and type a brief explanation of the error to alert the Delinea Expert development team. Your prompt and the resulting answer will become visible for analysis, along with your username and tenant name. (At this time, the Delinea Expert team will not contact you, but may develop that capability in the future.)

Known Issues

- **Missing Information:** Newly published documentation may sometimes not be available. Cause: Delinea Expert reviews all public documentation for Delinea products once per week.
- **Secret Server UI:** Instructions about the UI for Secret Server on Delinea Platform may be inaccurate, though the underlying principles are the same. Cause: Secret Server documentation is not always clear about the distinction between Secret Server On-Premises, Secret Server Cloud standalone, and Secret Server Cloud on Delinea Platform. This is being addressed manually by updating the Secret Server documentation.

Information Sources

Delinea Expert has access to the following sources:

- Delinea Platform documentation (where you're reading this)
- [Delinea Mobile](#) documentation
- [Secret Server](#) documentation
- [Web Password Filler](#) documentation
- [Connection Manager](#) documentation
- [Support Knowledge Base](#) (public only)
- [Delinea.com](#) (includes all blogs, whitepapers, and feature detail pages)

Access to Delinea Expert

By default, Delinea Expert is available to users and groups that have been assigned the built-in roles: **Platform User** and **Platform Admin**.

Some early customers were also given a role called **Delinea Expert** or **Custom Expert** that was applied to all users and admins.

To grant access to a set of users (such as Admins or IT Users) or to exclude a set of users (such as Business Users), simply check if their roles have the **Access Delinea Expert** permission.

1. Go to the platform's **Roles** page.
2. Check if the **Delinea Expert / Custom Expert** role exists and if it has been applied to any groups/users. You can remove the role from any groups that shouldn't have access.
3. If you have already created and assigned custom roles, you can edit them to remove the **Access Delinea Expert** permission from any role that should not have access.
4. Check whether the built-in roles **Platform User** or **Platform Admin** apply to any users or groups. To remove a group's access:
 - a. Duplicate the **User** or **Admin** role that you want to change.
 - b. Edit the duplicated role(s) to remove the **Access Delinea Expert** permission.
 - c. Reassign your groups to the new role(s).

If you do not want *any* of your users – including Administrators – to have access to Delinea Expert, contact Delinea Support or Sales to request deactivation of this feature.

If you have concerns about AI security, please see the next section.

Privacy & AI Transparency

Last Updated: August 6, 2024

AI Transparency Notice - Delinea Expert

Delinea Expert utilizes a private version of OpenAI GPT-4o hosted on Microsoft Azure to understand and generate human-like text using curated Delinea knowledge that is publicly available, including Delinea Docs (docs.delinea.com) and Knowledge Base articles (support.delinea.com).

All responses generated by Delinea Expert include reference links to the underlying sources for reference. This allows customers to review the source information by clicking the links embedded in the responses.

Frequently asked questions and answers are provided below. If you have further questions, please contact Expert@delinea.com.

Where are the Question Prompts and Responses Stored?

All customer prompts and responses are stored encrypted in the Delinea Expert specific platform database, separated per customer tenant. Customers can review their chat history by selecting the “Chat History” link in the Delinea Expert sidebar. Chats are retained in the Chat History until deleted by the customer.

Are Question Prompts Sent or Routed to “Open” or “Public” AI Models?

No. Customer prompts and responses do not leave the Delinea boundary and are stored encrypted in the Delinea Expert- specific platform database separated per customer tenant.

Does Delinea use Prompts for Fine-tuning or to Improve the Overall Responses?

No. Delinea does not use the prompts or responses for training or fine-tuning. However, customers do have the option of flagging a response for review by Delinea. If a response is flagged, a copy of the customer prompt and the response is stored in a dedicated Delinea Cloud Ops database for review by the Delinea development & documentation teams. This review could help improve both our documentation and answering mechanisms but will not be used to train or fine-tune the model.

Do Delinea Employees Have Access to the Prompts or Responses?

Only if the customer flags a prompt and response for review. In this case, the prompt and response will be reviewed by the Delinea development team.

Is Use of Delinea Expert Required?

No. Customers are not required to use the AI-driven expert and can always use the standard search bar or visit the documentation or support sites. Use of the Delinea Expert assistant is optional.

How were the AI-generated Search Results Tested?

Delinea teams began testing Delinea Expert in December 2023. During the initial test phase, Delinea input over 30K questions and tracked a reliability score of 99% based on closed loop feedback. While Delinea tested results to achieve high reliability, Delinea Expert can make mistakes and you should confirm important information, by visiting the citations links.

Does Delinea Expert Process Personal Data?

Delinea Expert is intended to answer questions, provide recommendations, and assist with technical inquiries related to Delinea's solutions. It was not designed to process personal data. The information and data entered into the Delinea Expert digital assistant is at the sole discretion of the customer. Please note that if a user submits feedback, Delinea will receive the user's name and email address for follow-up purposes.

Vaulting Secrets on the Platform

This page provides an overview of the Delinea Platform's core vaulting features and functions, which are built on the industry-leading technology of Secret Server Cloud.

For New Business Users

Secret Server has its own complete documentation set, and the information at the following link is specifically relevant to new, non-administrator users: [Secret Server End User Guide](#).

For New Administrators

The information at the following link is specifically relevant to new administrators: [Secret Server Cloud Quick Start](#)

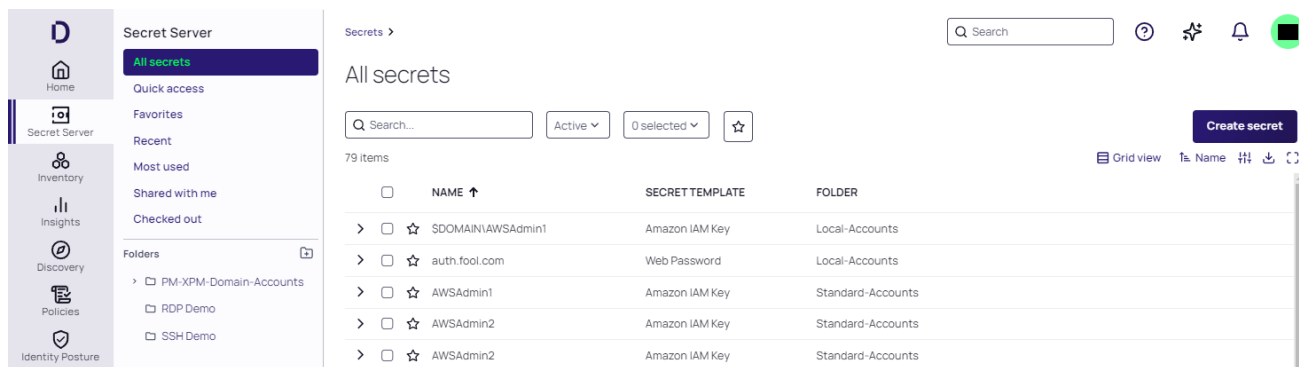
For Existing Secret Server Customers

On the Delinea Platform, secrets work the same way they work in Secret Server. The two systems share secrets and pinned folders, as well as administrative privileges, permissions, and access settings. Once you are logged in to the Delinea Platform, you will have the same access rights to secrets inside Secret Server as you did with the standalone Secret Server Cloud.

Accessing Secret Server from the Platform

To access Secret Server from the platform, simply hover over Secret Server in the left-side navigation.

Table of Contents



For more detailed information about the left-side navigation, please see [Delinea Platform Interface](#).

Secrets

Secrets are individually named packets of sensitive information, such as passwords. Secrets address a broad spectrum of secure data, each type represented and created by a secret template that defines the parameters of all secrets based on it. Secrets are very powerful and provide many ways of controlling and protecting their data. All secret text-entry field information is securely encrypted before being stored in the database, including a detailed audit trail for access and history. For more information about secrets, see the following pages in the Secret Server documentation:

- [Viewing Secrets](#) (includes checking expiration and history)
- [Deactivating and Reactivating Secrets](#)

Creating Secrets

You create a secret based on a secret template. There are many built-in specialized templates, with required fields that differ based on the purpose and type of secret you want to create. If you do not find a suitable template available, you can create a custom template.

For detailed information, see:

- [Creating Secrets](#)
- [Secret Configuration Options](#)
- [Editing Secrets](#) (includes manually changing passwords, instead of waiting for expiration)

Checking Out Secrets

The Secret Server *check-out* feature grants exclusive access to the secret for a single user for one or more pre-defined periods of time. No other user can access a secret while it is checked out, except for administrators with unlimited privileges. For more information about checking out secrets, see:

- [Checkout Overview](#)

Launching Secrets

Secrets are launched with tools named launchers. Launchers enable users to securely and conveniently access remote systems and applications using stored credentials without manually entering passwords. There are Remote Desktop Protocol (RDP) launchers for Windows sessions, SSH launchers for Unix systems, and web launchers for automatic website logins. You can also build custom launchers.

For detailed information, see:

- [Overview of Secret Launchers and Protocol Handlers](#)
- [Using Secrets on Websites](#) (Web Password Filler)

Secret Folders

Secret folders allow you to create containers for secrets, based on your needs. For example, you can use folders to organize secrets by customers, computers, regions, or branch offices. Folders can be nested within other folders to create sub-categories for each set of classifications. Secrets can be assigned to these folders and sub-folders.

You can customize permissions at the folder level so that each secret in a folder inherits the folder's permissions. Setting permissions at the folder level also ensures that future secrets added to that folder will all have the same permissions, greatly simplifying management across users and groups.

Creating Folders

To create folders, you must have a role with the "administer folder" permission. You also must have edit or owner permission for the parent folder. For detailed information, see [Creating Folders](#).

Moving Secrets Between Folders

To add or move a secret to a folder, you must have edit permission on that folder (either directly or through inheritance). When a secret is moved to a folder, it automatically gets the "Inherit Permissions from folder" setting, even if it had specific permissions before the move.

To move a secret from a folder, you must have edit permission on that secret. If the secret has the "Inherit Permissions from folder" setting enabled, you must have owner permission to move that secret to a new folder.

For detailed information, see [Adding and Moving Secrets Between Folders](#).

Credential Management

The Delinea Platform provides several features for credential management.

Discovery

Discovery is a powerful feature designed to help organizations discover and manage privileged accounts, credentials, and other sensitive information across their IT infrastructure. It enables IT teams to gain visibility into all of their systems, applications, and devices, and identify potential security risks and vulnerabilities.

By scanning and analyzing systems and applications, discovery can detect and classify privileged accounts and credentials, including those that are inactive or hidden. You can automatically find local Windows accounts, Active Directory services, Unix, VMware ESX/ESXi, and Active Directory domain accounts.

For more information about discovery, see the following:

Table of Contents

- [Discovery Overview](#)
- [Introduction to Discovery Sources, Scanners, and Templates](#)
- [Running and Interpreting Active Directory Discovery](#)

Distributed Engines

Secret Server distributed engines, or simply *engines*, are a powerful solution that enables organizations to manage privileged access across their entire infrastructure while maintaining security, control, and scalability. Organizations can scale their privileged access management infrastructure to meet the needs of large and distributed environments.

With engines, organizations can distribute the load of managing privileged accounts and credentials, allowing for faster response times and improved performance. They also enable organizations to maintain control over their sensitive data, with each instance of Secret Server being fully auditable and traceable.



Note: It is necessary to whitelist certificate CRLs if you have firewall rules in place. See [Architecture](#) documentation for [examples](#) about Secret Server Hybrid Multi-Tenant Cloud Architecture.

For more information about distributed engines, see [Distributed Engine Overview](#).

Remote Password Changing

Secret Server Remote Password Changing (RPC) is a credential rotation feature that enables IT teams to automatically change passwords for privileged accounts on remote systems and devices, without requiring direct access to those systems. This improves security and reduces the risk of security breaches caused by weak or compromised passwords. Organizations can automate changing passwords for privileged accounts on a schedule or in response to specific events. This includes local and domain accounts on Windows, Unix, Linux, and other systems, as well as service accounts, database accounts, and other types of credentials.

For more information about remote password changing, see the following:

- [Remote Password Changing Overview](#)
- [Automatic Remote Password Changing](#)
- [Understanding Expiration, Auto Change and Auto Change Schedules](#)

Auditing Privileged Account Activity

Secret Server provides a range of features for auditing privileged account activity, including:

- Advanced Session Recording
- Audit Logs
- Alerting and Notifications
- Reporting

Advanced Session Recording and Management

Secret Server Advanced Session Recording is a feature that allows organizations to monitor and record privileged sessions in real time. It provides an additional layer of security by capturing all user activity during privileged

Table of Contents

sessions, including commands entered, files accessed, and changes made to the system or application. It also enables IT teams to investigate security incidents and respond quickly to potential threats by providing a detailed record of user activity and enabling them to identify suspicious or unauthorized behavior.

With Advanced Session Recording, organizations can review session recordings for auditing purposes and use advanced search and filtering capabilities to quickly find specific events or actions. They can also configure policies to automatically trigger recording based on specific events or actions and limit access to session recordings to authorized personnel only.

For more information about advanced session recording, see [Advanced Session Recording Overview](#).

Audit Logs

Secret Server auditing is a feature that enables organizations to monitor and record all activities related to privileged accounts and credentials. It provides an additional layer of security by capturing detailed logs of all user activity, including login attempts, password changes, and access to sensitive data. Organizations can review audit logs and use advanced search and filtering capabilities to quickly find specific events or actions. Audit information is primarily available through reports and alerts. For more information, see [Secret Audit Log](#).

Alerts

Secret Server provides a range of alerts that can be configured to notify administrators of specific events or actions related to privileged accounts and credentials. Administrators can configure the alerts to be sent in email, SMS, or through a third-party system, and can set up different alerts for different users or groups. This helps organizations respond to potential security threats in real time and ensure that their privileged accounts and credentials are being used appropriately.

For more information, see:

- [Inbox](#)
- [Event Subscriptions](#)
- [Event Pipelines](#)

Built-in Reports

Secret Server includes many preconfigured reports that you can run or use as templates for creating custom reports.

For more information, see:

- [Configuring Session Recording](#)
- [Built-in Reports](#)

QuantumLock

The QuantumLock feature provides Safe Kyber protection for secrets. This protection is useful against risks from "Harvest Now--Decrypt Later" attacks and against risks associated with quantum computing.

You can reset a forgotten QuantumLock password using Platform MFA by following the steps below. You should already have MFA set up for your own authentication:

Table of Contents

1. From the left navigation menu, select **Settings**.
2. On the Settings page, choose the **Alphabetical** view.
3. Select **QuantumLock** below the letter, Q.
4. On the QuantumLock management page, select the **QuantumLocks** tab.
5. Select **Manage QuantumLock password**.
6. Select **Forgot QuantumLock Password**.
7. Select one of the authentication methods displayed.
8. Complete the authentication as indicated.
9. Click **Next**.
10. Enter and confirm a new QuantumLock password.
11. Click **Reset QuantumLock Password**.

Inventory

When you click **Inventory** from the left navigation menu, the options available vary, depending on the services you have chosen or not chosen, including Privilege Control for Servers (PCS), and ITP-PCCE.

- **Computers Inventory:** see "Managing Computer Assets" below
- **Remote Applications Inventory:** see [Accessing Remote Applications with PRA](#)
- **ITP-PCCE Inventories:** see "ITP/PCCE Inventory" on page 679 which include the following:
 - Access Policies
 - Activities
 - Assets
 - Groups
 - Identities
 - Memberships
 - Privileges
 - or any combination of the above.
- **Collections Inventory:**
 - see "Grouping with Computer Collections" on page 99
 - see "Collections" on page 704

Managing Computer Assets

The platform's Computers inventory provides an asset-centric view of all computers discovered using the Secret Server discovery service in one place—the Inventory page. From there you can efficiently manage and initiate

Table of Contents

remote sessions on your computer assets. To learn more about Secret Server's discovery service, see [Secret Server Discovery](#).



Note: Inventory is available only for Platform instances connected to Secret Server Cloud. It is not available for customers using the platform with Secret Server On Premises.

Inventory Permissions

User access to the computer inventory is controlled by permissions. Platform admins can assign these permissions to manage full or targeted access, either across all computers or within specific collections.

- To access computers from the Inventory menu in the platform's left navigation pane, users need the role permission View Inventory.
- To see all computers, users also need the role permission View All Computers.
- To give a user granular access to a set of computers, admins can make a collection and grant users permissions at the collection level. See ["Assigning User Permissions on Computer Collections"](#) on page 101.

Viewing Your Computers Inventory

Follow the procedures below to access a computer asset's basic and detailed information or launch a session into an asset.

Once Secret Server discovery has been enabled and configured, you can view your Computers inventory through the platform interface by selecting **Inventory** from the left navigation panel, then selecting **Computers**. The Inventory page displays a table with each computer asset in a row, and columns displaying basic information including the computer name, type, and domain. To adjust what data columns are displayed, click the column options icon just above the table on the right, and select or deselect boxes next to the column labels.

COMPUTER NAME	TYPE	DOMAIN	OPERATING SYSTEM	CLIENT VERSION	OPERATING SYSTEM NAME AND VERSION	CREATED DATE	LAST MODIFIED
LIN-SVR-01	Server		Linux		Red Hat Enterprise Linux	9/20/23, 10:43 AM	12/31/01, 6:30 PM
RAS-LINUX	Server		Linux		Red Hat Enterprise Linux	9/20/23, 10:43 AM	12/31/01, 6:30 PM
DC-2022	Server		Windows	6.0.1-362	Windows Server 2022 Datacenter Azure Edition	9/20/23, 10:43 AM	12/31/01, 6:30 PM
WIN-SVR-01	Server		Windows	6.0.1-360	Windows Server 2022 Datacenter Azure Edition	9/20/23, 10:43 AM	12/31/01, 6:30 PM
ENGINE-2022-2	Server		Windows	6.0.1-362	Windows Server 2022 Datacenter Azure Edition	1/18/24, 11:39 AM	12/31/01, 6:30 PM

Searching Your Inventory

You can search the inventory in two ways:

- Use the Search bar and filters
- Use the query builder

Using Search and Filters

To search for computers in the Computers inventory page, type some identifying text into the Search field at the top of the list. If you need to narrow down the search results further, choose values from the dropdown lists in the filters, such as Type. If the filter you want to use is not displayed, click **Add filter**.

Using Query Builder

Click **Show query builder** in the Computers inventory page to open the query builder. The query builder is an advanced search mechanism that you can use to create complex searches based on the information available. For more information, see "Using the Query Builder" on page 49.

Computers ☆ ↻

Allow users to view and launch remote sessions to computer assets identified by Secret Server Discovery. [Learn more](#)

Show filters

Computer Type

In

No values selected

AND

+

Search...

Server

Workstation

Clear query

Save as collection

183 items

Computer name

↑↓

⌵

Drilling into Details

If you click any empty space in a computer asset row, a panel opens on the right displaying details about the computer, such as the computer type, domain, DNS name, Active Directory OU, client version, and zone. The panel also displays links you can click to view more details or launch a remote session.

To see even more details, click the **Details** link in the panel. A page appears with more information about the selected computer. You can reach the same detail page by clicking the computer's name in the Inventory list. On the computer details page, the Details tab shows additional information, such as the preferred site and date the computer joined the zone.

The Policies tab (available to PCS customers only) shows which PCS policies include this computer as a target. See "Step 9: Set Up PCS Policies" on page 608.

The Audit tab presents an audit trail specific to that asset (**Computer Name**). You can find the same entries in the "Reviewing Audit Logs" on page 130, filtered by its **Target (Computer Name)**.

Computers >

Q Search

ⓘ ⚙️ 🔔 SB

Winsv-west57 ☆ ↻

Launch

Overview Policies Audit

Q Search

Date Last 7 days

×

Add filter

1 Date

⌵

⌵

111 items

DATE	SERVICE	LEVEL	ACTION
27/02/2025, 18:00	Secret Server	Security Audit...	Secret was viewed by Admin [redacted]
27/02/2025, 18:00	Identity	Security Audit...	Multi-factor authentication attempted by Admin [redacted]
27/02/2025, 18:00	Identity	Security Audit...	Login for user Admin [redacted]
27/02/2025, 18:00	Identity Protection	Security Audit...	Table cell content
27/02/2025, 18:00	Identity	Security Audit...	Table cell content
27/02/2025, 18:00	Identity Protection	Security Audit...	Table cell content
27/02/2025, 18:00	Identity Protection	Security Audit...	Table cell content
27/02/2025, 18:00	Identity Protection	Security Audit...	Table cell content
27/02/2025, 18:00	Identity Protection	Security Audit...	Table cell content
27/02/2025, 18:00	Identity Protection	Security Audit...	Table cell content

Logging In to a Computer

If you want to log in to (launch) a computer asset, click one of the launch options on the panel: **Launch with Secret**, **Launch with My Account**, or **Launch with Manual Credential**.

Launching with Secret

You can log on to any target system on the Delinea Platform by leveraging a vaulted credential from Secret Server. When selecting this option, vaulted credentials associated with that machine will appear and you will be prompted to select a secret to launch with.

Launching with My Account

You can log in to an enrolled Linux system with the same account you use to log in to the Delinea Platform, either from the platform or by using a native application that uses SSH, SCP, or SFTP.

Launching with Manual Credential

Selecting **Launch with Manual Credential** allows you to launch manually in to a target system with a valid username and password. Depending on how authentication rules and authentication profiles are configured for the system and account, you might be required to respond to additional authentication challenges before logging on.

Disabling Active Inventory |

To disable the inventory view, take the following steps:

1. Click **Settings** from the left navigation, then select **Administration** below Secret Server.
2. On the Secrets Administration page, click **Platform Integration** below Tools & Integrations. The Platform Integration page opens to the Configuration tab.
3. Click **Edit**.
4. Next to **Forward Inventory Data to Platform**, deselect the box. This action will prevent your tenant from incorporating newly detected computers. It will not impact any previously discovered computers.

PCS Policies

To meet your compliance requirements, you can assign policies precisely tailored to individual computers, ensuring that each asset operates securely and efficiently within your infrastructure. To learn more about assigning machine level policies, see PCS Policies.

For related content, see ["Grouping with Computer Collections"](#) below

Grouping with Computer Collections

You can save computer inventory queries as computer collections for future reuse. This provides better organization and management of assets. By using computer collections, you can:

- Avoid recreating the same queries daily
- Apply policies to specific subsets of your computer inventory

Computer collections are automatically updated every day through Discovery and can also be updated on demand.

Creating a New Computer Collection

1. Open the Computers inventory page (use the Search bar to find it).
2. Click **Show Query Builder**.
3. Enter your query terms. Results appear automatically on the page.
4. Click **Save as Collection**.
5. Enter a **Collection name** and **Description**.
6. Click **Save**.

The Collections page opens, displaying your new collection in the list.

To check the details of your new collection, click any empty space in the collection's row. A panel opens to the right displaying the details.

Modifying a Computer Collection

1. Open the Collections page (use the Search bar to find it).
2. Select the collection you want to modify.
The collection's detail page is displayed.
3. To modify the name or description:
 - a. Select the Overview tab.
 - b. Click **Edit**.
 - c. When finished, click **Save**.
4. To modify the query that determines which assets are in the collection:
 - a. Select the **Assets** tab.
 - b. Use the query builder to change the query.
 - c. When finished, click **Save**.

If you need to discard your changes, click **Reset**.

5. To modify the user permissions assigned to the collection, select the **Permissions** tab. See "Assigning User Permissions on Computer Collections" on the next page.

Deleting a Computer Collection

To delete a computer collection, you must have the Manage All Collections permission.

1. Open the Collections page (use the Search bar to find it).
2. Hover over the name of the collection you want to delete, and click the three dots to open the context menu.
Alternatively, you can click any empty space in the collection's row to open the preview panel.
3. Click **Delete**.

A confirmation dialog is displayed.

4. Confirm the deletion.

Assigning User Permissions on Computer Collections

By assigning permissions to users for computer collections, you can gain granular control over access to computer collections within your organization. You can specify permissions for individual users and groups, ensuring that only authorized personnel can view, manage, or interact with specific computer collections. By implementing this feature, your organization can enhance security, streamline access management, and ensure compliance with internal policies.

For more information about permissions, see ["Roles and Permissions"](#) on page 203.

To assign permissions on computer collections:

1. Open the Collections page (use the Search bar to find it).
2. Select the name of the collection for which you would like to assign user permissions.
The detail page for that collection is displayed.
3. Select the **Permissions** tab.
4. Click **Grant Access**.
5. On the Grant Access page, select users or groups to give them access to the collection.
6. Click **Next**.
7. Specify the permissions you would like your users to have on the assets within the collection, as well as on the collection itself. See ["Common Access Control Configurations"](#) on the next page and ["Permissions Reference"](#) on the next page.
8. Click **Assign**.
The **Permissions** tab of the Collections page is displayed, showing the members you selected and their permissions on the collection.
9. To modify permission assignments:
 - a. Click **Edit**.
 - b. Use the dropdown menu in each column to modify the selected permissions for each member.
 - c. Click **Save**.

Interaction Between Collection-Based and Role-Based Permissions

Collection-based permissions and role-based permissions are designed to work together.

Role-based permissions always override collection-level permissions. For example, if a user has the Launch permission at the role level, the user can launch into any machine to which they have access, as long as they also have the View Asset permission for that machine.

To control what a user can see or do at either the collection or asset level, follow these guidelines:

Table of Contents

- **Role-based permissions for viewing results:** To control what users can view, ensure they have the View Inventory permission at the role level. This grants access to inventory information across collections.
- **Collection-based permissions for collection access:** Permissions at the collection level govern which collections a user can view, access, update, or delete. To allow a user to view only a collection's results, but not the collection itself, assign the View Assets permission to the user. With the View Assets permission, the user can view the results within the collection without gaining access to the collection as a whole.
- **Granular access:** To gain finer control over what a user can access, you can combine role-based and collection-based permissions. For example, you can grant the user View Inventory permission at the role level, but only grant the View Assets permission at the collection level. The user can view asset data, but not the collection structure itself.

Common Access Control Configurations

To grant a user access to view only a subset of computers in the Computers inventory, give the user the following permissions:

- Role permission: View Inventory
- Collection permission: View Assets

To grant a user access to launch a session to any computer within an assigned collection, give the user the following permissions:

- Role permissions: View Inventory, Launch PRA Session
- Collection permission: View Assets

To grant a user access to view both the collection and the collection results in the Computers inventory, give the user the following permissions:

- Role permission: View Inventory
- Collection permissions: View Assets, View Collection

To grant a user the ability to manage a collection, including updating its query, give the user the following permissions:

- Role permission: View Inventory, Manage All Collections

To grant a user access to assign collections to policies, which enables the user to update the policy, give the user the following permissions:

- Role permissions: View Inventory, Edit Policy
- Collection permission: View Collection



Note: To enable the user to view all collections, Assign View All Collections at the role level.

Permissions Reference

The following table gives a summary of the role permissions.

Table of Contents

Role Permission	Description
View All Collections	User can view details for all collections in the platform tenant
Manage All Collections	User can create, view, update, and delete all collections in the tenant
Launch with PRA	User can launch remote access on supported assets
View All Computers	User can view all computers in the inventory
View Inventory	Must be enabled for the user to view any Inventory results

The following table gives a summary of the collection permissions.

Collection Permission	Description
Permissions to a Collection	
View Collection	User can view the overview tab of a collection
Grant Access	User can grant and manage access to a collection
Update Collection	User can update Collection Query, Name, and Description
Delete Collection	User can delete a Collection
Permissions to Assets in a Collection	
View Assets	User can view Collection results in Inventory
Launch Session	User can launch a session to collection results in Inventory

ITP/PCCE Inventory

For both Identity Threat Protection and Privilege Control for Cloud Entitlements, Inventory pages provide a centralized and comprehensive view of all identities, access privileges, assets, and activities across an organization's cloud services and applications. This visibility is essential for detecting and mitigating identity risks and active threats, ensuring compliance, and maintaining a secure access baseline.

Inventories enable organizations to:

- **Detect and Eliminate Over-Privileges:** By having a detailed inventory of access privileges, organizations can identify and mitigate over-privileges based on granular usage data and AI-based recommendations.
- **Monitor for Misconfigurations and Exposed Resources:** Inventories help in detecting risky misconfigurations such as exposed Git repositories and stale file access on shared drives, thereby hardening the identity security posture.

You can use inventories to do the following:

Table of Contents

- Gain a holistic view of all the connected applications, their users, and access.
- Identify important issues across your organization like stale cloud service accounts and users without MFA.
- Define Collections that can later be reused for other product features such as security rules and reports.

The inventory pages display information that was either gathered from integrated systems or entered manually and then processed.

Inventory Types

ITP/PCCE inventories are displayed on the following pages:

- **Identities**: Displays identities and accounts.
 - **Identity**: A unique identity (human or nonhuman) that owns one or more cloud service accounts. A nonhuman identity could be a machine identity, an automatic identity, or any other identity that doesn't belong to a human.
 - **Account**: A unique account (human or nonhuman) in a single application. A nonhuman account might be a service account, a workload, or even a user account that is used for automated tasks.
- **Groups**: Displays entities that define permissions granted to multiple accounts. This could be an IdP group (like a group of engineers who use the same design tools to build their product or application) or an AWS role that grants the same permissions to similar actors. The Groups table displays the applications in which the groups are managed, not the applications to which those groups grant access.
- **Assets**: Displays every object in integrated systems to which users can be granted access, like files, folders, databases, virtual machines, and applications.
- **Memberships**: Displays all groups and their members. For example, if a group represents the Engineering department, the Membership inventory presents all its members. You can use this page to find the relationship between groups and their members, such as all groups a specific person belongs to.
- **Access Policies**: Displays effective access and effective permissions. Effective access represents the permissions an entity (for example, a user) has on another entity (for example, an asset), based on what access was granted. Effective permissions are the combination of direct and indirect permissions used when accessing an object. You can use this page to find the relationship between an entity (cloud service user or group) and an asset.
- **Privileges**: Displays a list of all privileges at all levels.
- **Activities**: Shows actions taken by various identities, and when each action was done.


Inventories User Interface

To access inventories, click **Inventory** from the left navigation menu of the Delinea Platform. Select one of the choices from the secondary menu, such as Identities.


Table of Contents







Identities

AWS Users Enabled/Unknown Status Users +

+ 

Group By ▾

Showing 51,073 Identities Columns **Identities** Accounts 

<input type="checkbox"/> Identity	Source Apps	Access To Apps	Incidents ↓	Tags
<input type="checkbox"/>  Taylor Watts			8	-
<input type="checkbox"/>  Crystal Lewis			8	-
<input type="checkbox"/>  Shannon Leon...			8	-

Searching by Custom Properties



You can search by custom application properties, such as subscriptions in Azure or public repositories in GitHub or GitLab. This enables you to better scope the results based on your unique organizational values.

Custom properties are added by:

- **The Delinea Platform:** Each built-in integration exposes a set of custom properties. While custom properties retain the naming from their source, some imported properties are normalized on the platform with standard names.
- **Users:** You can add custom properties (when building a custom integration) that enable you to import and search by any property from the source application.

Sorting the Inventory Table

Each inventory table has a default sort order, indicated by the dark arrow displayed in the column header:

Identity ↑	Source Apps	Access To Apps	Incidents ↑
			
Current sort			Potential sort

To change the sort order, hover the pointer over a column header. When a dimmer arrow is displayed, you can click it to change the sort order.

Using Other Views

In addition to the Inventory table, most inventory items also have a single-entity view and a quick view.

Single-Entity View

To see more information about an inventory item, open its single-entity view by clicking either the entity name (leftmost table column) or the target name (in Access Policies, Membership, and Activities tables).

The single-entity view shows much more information about the inventory entity; for example, top incidents and MITRE tactics. You can investigate further using the Access Explorer.

Quick View

When you hover over the entity name, a quick view is displayed. The quick view shows a short list of commonly needed information. You can also investigate in the Access Explorer, show the entity in the source app (in some cases), and show the single-entity view.

Configuring Table Columns

You can customize the presentation of tables in the following ways:

- Choose which columns are displayed
- Resize the column widths
- Change the order of the columns

These options are available in all inventory tables. Your choices are relevant to the specific page where you made the choices and will persist through future login sessions.

To set the displayed columns:

1. From an inventory table, click **Columns** above the table. The list of available columns is displayed.
2. To display a column, select it. To hide a column, clear its selection. The column display adjusts immediately. If a column name is dimmed, it cannot be hidden.

To set the column width:

1. From an inventory table, point the cursor between column headings where you want to adjust the width until the cursor changes to multiple arrows.
2. Drag the cursor left or right to adjust the column width.

To set the column order:

1. From an inventory table, point the cursor at a column you wish to move. The gray column dividers on both sides are displayed.
2. Drag and drop the column to its new position.

Exporting a Table as CSV

You can download a file in CSV format containing all information displayed on an inventory page. If the download is limited to a certain number of entries, that limit is displayed when hovering over the download icon. To download more entries than the limit allows, filter the table to sets with fewer than the maximum number of entries, then download each set separately.

Using Tags

Tags are descriptive keywords (metadata) attached to data so you can find the data by browsing or searching. Tags are displayed in inventory tables and in the single-entity view. To get more information about any system tag, hover your cursor over the tag to read an explanation.

When an application is integrated with the platform, entities tagged in the source system are similarly tagged in the platform. In some cases, the platform also applies its own tags.

You can apply tags manually from most inventory pages (except the Membership and Access Policies pages) or from the single-entity view. You can apply existing tags or create new tags. You can apply tags to one or multiple entities simultaneously.

To apply existing tags in an inventory page:

1. Select the row you want to tag.
To apply the same tag to multiple rows, select multiple rows.
2. Click **Add Tags**, then click **Add tags** again.
3. To apply an existing tag, select the tag, then click **Save**.
You can search for tags by typing the first few letters.

To create and (optionally) apply new tags in an inventory page:

1. Select an inventory row.
If you intend to apply your new tag at the same time you create it, select one or more rows.
2. Click **Add Tags**, then click **Add tags** again.
3. Type a new tag name.
4. Click **Add New**.
5. (Optional) To apply the new tag, click **Save**.
If you do not apply the tag, the new tag is still created. It can be applied to entities later. You can apply both existing and new tags in the same step.
6. To add more new tags, type another new tag name and click **Add New**.

Filtering an Inventory Table

By default, each inventory page includes a table displaying all data relevant to the page. You can filter the table to show only the data you are interested in, creating granular queries to understand the inventories, groups, and assets in your Delinea Platform environment. For example, you can display all the identities with admin privileges whose cloud service accounts were disabled or suspended (or are unknown).

For more information about how to use basic and advanced filtering, see ["Filtering in List Pages"](#) on page 48.

For more information about the filter fields for each inventory, see ["Inventory Filter Properties"](#) below.

Inventory Filter Properties

This section is a reference to all the filter properties provided by the Delinea Platform in the Inventory pages.

Identities

Category	Property	Description
Account	Access To Apps	The applications a cloud service user (or service account) can access. The access might be direct or indirect (such as federated access).
	Admin Access	Cloud service user accounts with administrative privileges. You can specify the application for which you want to find users with admin access. To modify this setting, select Settings > Authorization Configuration .
	Blast Radius Risk	Impact of an account to be taken over, based on the account's access and type of access.
	Email	Email of the cloud service user (or service account) as found in the application.
	First Name	First name of the cloud service user (or service account) in an application. The First Name may vary from application to application.
	ID	ID
	Incidents Count	The number of incidents an account has (for example, the incidents in the AWS account).
	Is External	Find accounts that are external (or not external). External accounts are based on the email and properties of the account being different from internal users (or as stated in the downstream application).
	Is Managed	A managed account is managed by the current system's administrator. Use this filter to find all accounts your administrators have full control over, or those they do not control that have access to your systems.
	Is MFA Enabled	Find applications where MFA is set (or not set). MFA settings may be different in different accounts; for example, MFA might be enabled in Okta but disabled in Slack.
	Last Login At	Date of the last login in a specific application.
	Last Name	Last name of the cloud service user or service account. The Last Name may vary from application to application.

Table of Contents

Category	Property	Description
	Overall Risk	The overall risk is calculated based on the probability that an account can be taken over and the blast radius risk (defined earlier in this table).
	Detection Rule Name	Cloud service users who match a specific detection rule; for example, finding all the users that matched the brute force attack.
	Privileged Access	Cloud service user accounts with privileged access. You can select the application to identify users with privileged access. To modify this configuration, select Settings > Authorization Configuration .
	Shadow Admin Access	Cloud service user accounts with shadow-admin privileges across various applications. You can choose the specific application for which you want to find users with shadow-admin permissions. Shadow-admin permissions grant users administrative capabilities with a reduced set of permissions they currently possess.
	Source App	The application in which the account is a registered cloud service user. For example, if a user has federated access to AWS through an IDP (such as Okta), Okta is the source app, and AWS is found in the Access to app filter.
	Status	The status of the account in the source application, such as Deleted, Disabled, Enabled, or Unknown.
	Sub Type	All the available sub-types of non-human Identities.
	Tags	Tags that are associated with the account (such as Admin, Privileged Access). Tags are created automatically by the AI engine, manually by the end user, or are based on tags in the source system.
	Take Over Risk	The probability that an account will be taken over by an external identity.
	Type	User or Service Account
Collection	Name	The named Collection is used as a filter. All collection types can appear in the filter. If an Access-type collection is used, then the identities that matched will be returned.

Table of Contents

Category	Property	Description
Identity	Blast Radius Risk	Identities are filtered based on the risk imposed by their access collection. This filter focuses on the highest Blast Radius among all related accounts, providing insights into the extent of potential damage in case of a security breach. With this filter, you can quickly locate critical accounts or high-risk cloud service users with extensive access permissions. Use this filter to prioritize security measures and reduce the overall risk of breaches.
	Department	The department in which the identity works (for example, Customer Support, Sales, HR).
	First Name	The first name of the identity. Taken from the primary account of the identity, which is often the HR system or the IdP.
	Hired At	Date hired.
	Last Name	The last name of the identity. Taken from the identity's primary account, which is often the HR system or the IdP.
	Manager	The name of the identity's manager.
	Name	The name of the identity, which is either taken directly from the primary account of the identity (the HR system or IdP in most cases) or a combination of the First and Last names from the Primary account.
	Overall Risk	Comprehensive risk of an identity, considering the combined risks of its individual accounts. Incorporates two main components: Account Takeover Risk, which gauges the vulnerability of the identity to unauthorized access, and Blast Radius, representing the highest scope of permission the identity can achieve. Use this filter to search for identities with significant security concerns, prioritizing measures to mitigate potential breaches and safeguard sensitive data.
	Source Apps	All applications for which the identity has a registered user account. For example, if a user has federated access to AWS through an IdP (such as Okta), only Okta will be represented as the source app, and AWS will be in the Access to App filter.
	Tags	Tags associated with the identity (such as Senior Employee, Involved in Credential Leak, Finance Employee). Tags are created automatically by the AI engine or manually.

Table of Contents

Category	Property	Description
	Take Over Risk	The ease with which an attacker could gain access to any of an identity's connected accounts. This filter assesses the risk level posed by each individual account, providing a comprehensive understanding of the identity's overall security vulnerability. By utilizing this filter, you can identify identities with weak account security, so you can prioritize security enhancements and protect against potential unauthorized access and data breaches.
	Terminated At	Terminated At
	Title	The job title of the identity (such as CTO, Software Engineer).

Groups

Category	Property	Description
Group	Admin Access	User accounts with administrative privileges. You can specify the application for which you want to find users with admin access. To modify this setting, select Settings > Authorization Configuration.
	Alternative Name	The alternative name of the group is presented to users and reviewers across the platform alongside the group name and is used to provide a clearer name for of the group
	Collections	The named Collection is used as a filter. Filtering is based upon the results of the Collection query in this inventory. The filter result shows all the groups that matched the Collection.
	ID	ID
	Incidents Counts	The named Collection is used as a filter. Filtering is based upon the results of the Collection query in this inventory. The filter result shows all the groups that matched the Collection.
	Is Empty	Empty groups or non-empty groups.
	Name	The name of the group as stated in the source system.
	Origin Type	The type of the group in the source application (such as AWS Role or Salesforce Profile).
	Owner	The name of the owner of the group, if any.

Table of Contents

Category	Property	Description
	Detection Rule Name	Filter based on groups that matched a specific detection rule. For example, find groups that grant admin access.
	Privileged Access	User accounts with privileged access. You can select the application to identify users with privileged access. To modify this configuration, select Settings > Authorization Configuration .
	Shadow Admin Access	User accounts with shadow-admin privileges across various applications. You can choose the specific application for which you want to find users with shadow-admin permissions. Shadow-admin permissions grant users administrative capabilities with a reduced set of permissions they currently possess.
	Source App	The app on which the group is managed.
	Tags	Tags associated with the group (for example general, birthright group). Tags are created automatically by the AI engine, manually, or are based on the tags in the source system.

Assets

Category	Property	Description
Asset	Created At	Creation date of the asset, if available.
	Collections	The named Collection is used as a filter. Filtering is based upon the results of the Collection query in this inventory. The filter result shows all the Assets that matched the Collection.
	ID	ID
	Incidents Counts	The number of incidents associated with the asset.
	Last Used At	The last time the asset was used (accessed, modified, deleted or created). This data is available mainly for Secrets and Applications, and is not available in most other asset types.
	Name	Name of the asset.
	Origin Type	The type of the asset on the source application (for example: EC2 machine in AWS, or Application in Okta).
	Detection Rule Name	Filter based on assets that matched a specific detection rule. For example, find production assets that can be accessed by non-admins.

Table of Contents

Category	Property	Description
	Source App	The app on which the asset is managed.
	Tags	Tags associated with the asset (for example, Production or Test Environment).
	Type	Assets are "normalized" (grouped) to a minimal set of types across all applications. Assets can therefore be filtered by their "normalized" Type (such as Virtual Machine), and they can be filtered specifically by the name of the asset in the source system (for example, EC2 machines on AWS).

Memberships

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities - Account	See "Identities" on page 108.
	Identity	Collection	Same as Identities-Collection	See "Identities" on page 108.
	Identity	Identity	Same as Identities - Identity	See "Identities" on page 108.
	Group	Group	Same as Groups inventory	
Target	Group	Group	Same as Groups inventory	
Access		Membership	Added at	Date when this membership was created.
			Added by	Person who created this membership.
			Direct Access	Direct Access
			Collections	Collections

Access Policies

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities -Account	See "Identities" on page 108.
	Identity	Collection	Same as Identities -Collection	See "Identities" on page 108.
	Identity	Identity	Same as Identities -Identity	See "Identities" on page 108.
	Group	Group	Same as Groups	
Target	Asset	Asset	Created At	Creation date of the asset, if available.
			Collections	The named Collection is used as a filter. Filtering is based on the results of the Collection query in this inventory, so the results will be all the Assets that matched the Collection.
			ID	ID
			Incidents Count	The number of incidents associated with the asset.
			Last Used At	The last time the asset was used (accessed, modified, deleted or created). This data is available mainly Secret or Applications assets, and is not available in most other asset types.
			Name	Name of the asset.
			Origin Type	The type of the asset on the source application (for example: EC2 machine in AWS, or Application in Okta).
			Detection Rule Name	Filter based on assets that matched a specific detection rule. For example, find production assets that can be accessed by non-admins.
			Source App	The app on which the asset is managed.

Table of Contents

Filter	Entity Type	Category	Property	Description
			Tags	Tags associated with the asset (for example, Production or Test Environment).
			Type	Assets are "normalized" (grouped) to a minimal set of types across all applications. Assets can therefore be filtered by their "normalized" Type (such as Virtual Machine), and they can be filtered specifically by the name of the asset in the source system (for example, EC2 machines on AWS).
Access		Access	Collections	The named Collection is used as a filter. Only Access Collections will yield results in this inventory.
			Granted at	Date when the access policy was created.
			Granted by	Person who created the access policy.
			Is Direct	A direct assignment of access is any access granted to the account/group directly and not through another group. When marked as Yes, only direct access will be shown and calculated in the result. When marked as No, not only indirect will be included. To include both options, do not use this filter.
			Last Used At	Date when the access policy was most recently used.
			Limit Inheritance	Include only the first asset in the system that matches the query. Does not return any inherited assets. For example, if you want to find administrative access in a file system, and a user has access to a folder that contains a file, this filter returns only the folder.

Table of Contents

Filter	Entity Type	Category	Property	Description
		Privilege	Is Role	Privileges of a role on different assets. Different users get the same privilege (through the same role), but on different assets. In the platform, this is called a local role.

Privileges

Category	Property	Description
Privilege	Child Privileges	Privilege that contains a specific child privilege. For example, search the privilege Add MFA and find every admin or similar role that can add MFA devices.
	Is Role	Filter on whether privilege represents a role on the application.
	Origin Name	The name of the privilege in the source application.
	Source App	The app on which the privilege is managed.
	Tags	Tags associated with the privilege (for example, Production or Test Environment).
	Type	Privileges are "normalized" (grouped) to a minimal set of types across all applications. Privileges can therefore be filtered by their "normalized" Type (such as Administrative), and they can be filtered by the name of the privilege in the source system (for example, ORG.ADMIN on GitHub).

Activities

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities - Account	See "Identities" on page 108.
	Identity	Collection	Same as Identities - Collection	See "Identities" on page 108.
	Identity	Identity	Same as Identities - Identity	See "Identities" on page 108.
	Group	Group	Same as Groups	

Table of Contents

Filter	Entity Type	Category	Property	Description
Target	Asset	Asset	Same as Access Policies - Target - Asset	See "Assets" on page 112.
	Identity	Account	Same as Identities - Account	See "Identities" on page 108.
	Identity	Collection	Same as Identities - Collection	See "Identities" on page 108.
	Identity	Identity	Same as Identities - Identity	See "Identities" on page 108.
	Group	Group	Same as Groups	
Privilege		Privilege	Child Privileges	Privilege that contains a specific child privilege. For example, search the privilege Add MFA and find every admin or similar role that can add MFA devices.
			Is Role	Filter by whether the privilege represents a role on the application.
			Origin Name	The name of the privilege in the source application.
			Source App	The app on which the privilege is managed.
			Tags	Tags associated with the privilege (for example, Production or Test Environment).
			Type	Privileges are "normalized" (grouped) to a minimal set of types across all applications. Privileges can therefore be filtered by their "normalized" Type (such as Administrative), and they can be filtered specifically by the name of the privilege in the source system (for example, ORG.ADMIN on GitHub).

Filter	Entity Type	Category	Property	Description
Activity		Activity	Date	The date when the activity was performed.
			Is Virtual	Filter on whether an activity is virtual. Virtual activities are activities that are not logged in the external system but are represented as activities in the platform, such as login events.
			Success Status	Success Status
			Tags	Tags associated with the activity.

Insights

Delinea Insights provides the core services for security and analytics. These include:

- "Reviewing Audit Logs" on page 130
- "Reviewing Session Recordings" on the next page

AI-Driven Auditing (AIDA)



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

AIDA (AI-Driven Audit) automatically reviews privileged SSH and RDP recordings with computer vision and large language model (LLM) analytics. It turns hours of video into a searchable audit trail, pinpointing elevated commands and risky behavior so PAM, security and audit teams can find answers in seconds.

Data Privacy and Processing

Delinea uses Azure Computer Vision (ACV) and Azure OpenAI, both services provided by Microsoft, to enhance our offerings. Key data handling and privacy features include:

- Regional Data Hosting: All data is hosted and processed within the same region that you have selected for your cloud operation, ensuring compliance with regional data handling regulations.
- Data Deletion After Processing: When Azure Computer Vision and Azure OpenAI finish processing data from a Delinea Platform session recording, the data is immediately deleted from Azure and not retained by Microsoft. This ensures that evaluation data is handled securely and transiently.

- **No AI Training with Customer Data:** Delinea does not use customer recordings or data to train AI models. We are committed to ensuring that customer data is used strictly for the purpose of delivering the services requested and maintaining privacy and integrity.

Session Recording

- The Session Recording page lists every captured session, live or completed and shows which ones have already been analyzed by AIDA. For analyzed sessions, you'll see AI-generated labels, and a one paragraph summary. A label filter lets you instantly surface sessions containing specific actions (e.g., **Privilege Elevation** or **IAM**).
- See "Analyzing a Recording with AIDA" on page 126 for details regarding analyzed sessions.
- Recordings and analysis are based on three synchronized data streams:
- Visual frame OCR - High resolution screen shots processed with OCR to read on-screen text (commands, output, file paths, SQL queries, etc.)
- Keystroke log - Time stamped command input with window focused context
- Process trace - Background processes spawned during the session for full situational awareness.

Reviewing Session Recordings

Session Review provides an additional level of security by recording a user's actions after a session is launched.

The Delinea Platform captures second-by-second screen shots in the browser during a user's recorded session. These images of the user's screen are compiled into a video that can be played back for auditing and security purposes.

Session Review allows administrators with the appropriate permission to view all active launched sessions within the platform. If Session Review is enabled on the secret, an administrator can watch the user's session in real time or after the session recording has been completed.



Note: Recordings listed in the Session Review table that are sourced from Secret Server On-Premises systems are not supported for viewing or analysis. Playback is only supported when requested from the same network as the secret-server On-Premises installation.

Enabling Session Review

Before you can view session recordings on the platform, a session recording must be configured within the vault on both the tenant and secret level. See [Configuring Session Recording](#) to configure Session Recordings within your Secret Server Cloud instance.

Launching a PRA Session with Session Review Enabled

Confirm that a secret has session recording enabled. Select the secret and navigate to the **Security** tab. In the Other Security section of the page, the **Session Recording Enabled** field indicates enabled.

Table of Contents

The screenshot shows the 'Check Out' and 'Approval' sections of the Delinea Platform interface. The 'Check Out' section has a table with columns for 'Require Check Out' and 'Edit'. The 'Approval' section has a table with columns for 'Require Approval Type' and 'Edit'. The 'Multifactor Authentication' section has a table with columns for 'Require Multifactor Authentication' and 'Edit'. The 'Password Requirements' section has a table with columns for 'Validation' and 'Password'. The 'Other Security' section has a table with columns for 'Require Comment', 'Enable Double Lock', 'Session Recording Enabled', and 'Hide Launcher Password'.

Require Check Out	Edit
No	

Require Approval Type	Edit
No	

Require Multifactor Authentication	Edit
No	

Validation	Password
Do not validate on Create (Do not validate on Edit)	Default (Template)

Require Comment	Enable Double Lock	Session Recording Enabled	Hide Launcher Password
No	No	No	No

On the **Overview** tab, under Launchers, select **Open with Remote Access** to start a remote access session to the target machine.

The screenshot shows the 'Details' and 'Launchers' sections of the Delinea Platform interface. The 'Details' section has a table with columns for 'Secret Name', 'Secret Template', 'Domain', 'Username', 'Password', and 'Notes'. The 'Launchers' section has a table with columns for 'Launcher' and 'No Active Sessions'. The 'Expiration and Heartbeat' section has a table with columns for 'Expiration' and 'Last Heartbeat Status'. The 'Advanced Information' section has a table with columns for 'Folder', 'Secret Policy', and 'Site'.

Secret Name	Secret Template	Domain	Username	Password	Notes
gm-spm-local-john-melody	Active Directory Account	gm-spm-local	john-melody	*****	None

Launcher	No Active Sessions
RDP Launcher	
Open with Remote Access	

Expiration	Last Heartbeat Status
Expired 27 days ago (Expires every 30 days)	Unknown Error - 15 days, 17 hours ago

Folder	Secret Policy	Site
Standard Accounts	Domains from Folder: None	Prod Office Oregon

Enabling Metadata Recording

By default, session recording creates videos of the launched session. In addition to video, the Delinea Platform supports logging additional metadata, such as keystrokes for RDP and SSH sessions. When these options are enabled, users can search for keystrokes or applications across sessions, and the session playback interface shows additional activity information.

Remote Desktop session metadata requires Secret Server 10.6 and the advanced session recording feature. This feature requires installation of Secret Server's advanced session recording agent (ASRA), or Direct Audit agent on the target servers. See [Installing the Advanced Session-Recording Agent](#).


SSH keystroke data relies on the Secret Server SSH Proxy. To enable SSH Proxy, see [SSH Proxy Configuration](#).

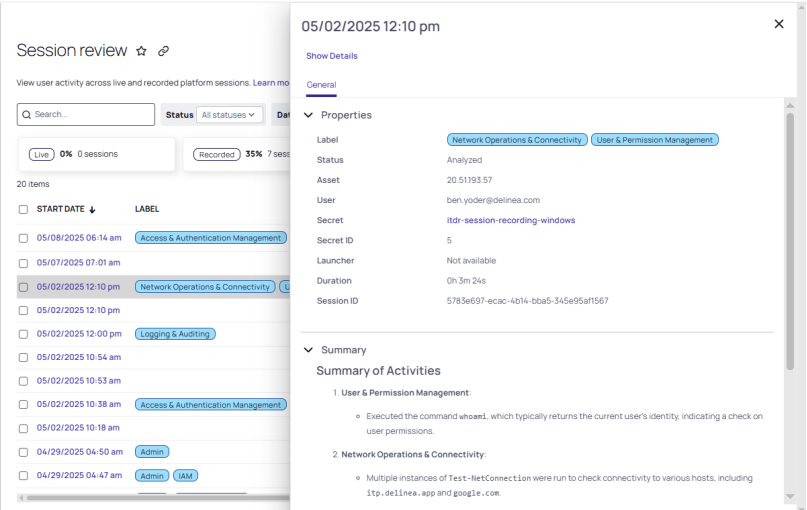
When the proxy is enabled, recorded SSH sessions log SSH traffic, which can be searched and displayed in the Session Recording playback interface. See "Viewing Sessions" on the next page.

Viewing Sessions

When you view the Session review page for the first time, it lists each session you have access to (the Delinea Platform and other native sessions).

- Click on the hyperlinked **Start Date** field to view the associated recordings on the Session Recordings page.
- Click on any field that is not a hyperlink to display the Details page for that session. Details include Properties, and if analyzed, a Summary (narrative of video events).


 **Note:** Recordings listed in the Session Review table that are sourced from Secret Server On-Premises systems are not supported for viewing or analysis. Playback is only supported when requested from the same network as the secret-server On-Premises installation.



The values displayed in the columns are sortable and configurable. Click the column headers to sort; click the Displayed Columns icon (≡) to control which columns of data are displayed.

Parameter	Description
Activity	Any activity detected in the session. Categories include: Anomaly - activity that deviates from the norm Keystroke - client keystroke activity Process - application executions on the endpoint
Start Date	The time and date when the remote session was initiated.
Session ID	The unique numeric identifier assigned to each session by the Delinea Platform for tracking.

Table of Contents

Status	<p>Session recordings go through the following lifecycle:</p> <p>Live: This is an active session. You can view a live stream of the remote session in near real time.</p> <p>Recorded: When the session encoding is successfully completed, the final recording is available to review.</p> <p>Finished: The session was completed, but session recording was not enabled for viewing.</p> <p>Failed: Any session that has not completed recording or encoding.</p> <p>Analyzed: The video was transcribed and analyzed by Delinea AI to detect risk.</p> <p> Note: Use the All Statuses dropdown list to limit the display of recording to a particular status.</p>
Source	The service from which the remote session was launched.
User	<p>The username of the user who launched the remote session.</p> <p>Click an available USER link to view that user's "Managing User Accounts" on page 179.</p>
Launcher	The various methods or triggers used to initiate session recordings.
Secret	<p>The vaulted secret used to launch the remote session. A user can drill down into the secret directly to view additional details about the secret, assuming the user has the required permissions.</p> <p>Click an available SECRET link to view its secret key information on Secret Server.</p>
Secret ID	The unique identifier for the secret.
Asset	The asset recorded, such as a server name or an IP address. The asset represents the target machine that the user remotely accessed using the Remote Access Server in the Delinea Platform.
Duration	This is the total time recorded for the session.
Label (AIDA only)	Labels are only available with AIDA (). AIDA tags each command identified in the session with one or more high-level labels so you can filter and pivot data quickly.

Label (AIDA)	Description
Administrative	Manage system settings or user roles
Authentication	Handle user log in, log out, or credential
Backup & Restore	Back up data or trigger restores
Cloud & Remote Services	Connect to or administer cloud/remote systems

Table of Contents

Data Analysis & Visualization	Inspect logs or metrics; generate on-screen reports
Development & Compilation	Build code or privileged scripts
File Operations & Transfer	Copy, move, delete, or sync files
File Directory Management	Create, rename, or protect folders; set permissions
IAM	Provision, modify, or revoke identities and roles
Logging & Auditing	Read or export security logs
Network Ops & Connectivity	Configure networks or monitor traffic
Package Management	Install, update, or remove software packages
Performance Optimization	Tune system or application performance
Privilege Elevation	Gain or monitor elevated privileges (e.g., sudo)
SSH Key Management	Create, rotate, or distribute SSH keys
Security & Encryption	Configure security controls or encryption
Shell & Script Operations	Execute or automate shell scripts
Software Build & CI/CD	Deploy or manage CI/CD pipelines
Storage & Disk Management	Manage disks, volumes, or storage pools
Suspicious	Match known attack patterns or risky behavior
System Info & Monitoring	Gather system-health or status data
System Mgmt & Configuration	Configure services or OS settings
Text Processing & Search	Search or manipulate text/log files
Troubleshooting & Diagnostics	Diagnose and resolve issues
Virtualization & Containers	Manage VMs, containers, or orchestrators

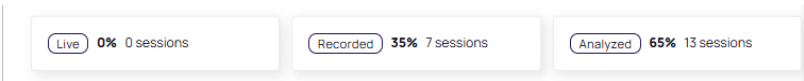
Searching and Filtering Sessions

The Session review table allows you to focus on specific recordings using the following search and filter features.

Status cards

Status cards display statistics, in percentage of total sessions. Click any card at the top of the table to quickly filter the table for that status.

Table of Contents



Search

Use the Search field to search content in any of the columns.

Filter

Select **Add filter** to choose additional filter criteria. When you pick a filter field from the dropdown list, a card appears at the top of the table, with a dropdown list of options.

You can filter by status, specific data, or any combination of displayed columns. Limit the results to a specific date range using the **Date** filter.

Session review ☆ ⓘ

View user activity across live and recorded platform sessions. [Learn more about session review](#)

Search: [Q Search] ⓘ ⚙ ⚪ KD

Filters: Status: All statuses ▾ Date: Last 30 days ▾ Secret: Any Secret ▾ x Add filter

Summary cards: Live 0% 0 sessions, Recorded 29% 4 sessions, Analyzed 71% 10 sessions

14 items

<input type="checkbox"/> START DATE ↓	LABEL	STATUS	ASSET	SECRET
<input type="checkbox"/> 05/08/2025 06:14 am	Access & Authentication Management +6	Analyzed	10.14.0.5	pra.itp.delinea...

Filter dropdown menu: Activity, Asset, Label, Launcher, Source, User

For more information, see "Filtering in List Pages" on page 48.

Viewing Session Recordings

Select any session or group of sessions with recordings on the Session review page. All sessions in the recording are displayed in the Session Review panel. Click any card in the panel to view the associated recording in the video player.

See "Analyzing a Recording with AIDA" on page 126 for details on analysis.

Table of Contents

The screenshot displays the Delinea Session Review interface. At the top left, there is a 'Session review >' link. The main area is divided into several sections:

- Video Player:** A large video player showing a session recording. It includes a progress bar at the bottom with a play/pause button, a full screen button, and a settings icon. The video title is '05/02/2025 12:10 pm' with a 'Recorded' status.
- Activity:** A section on the right side of the video player. It features a search bar, a 'Delinea AI can generate a transcript for this session recording. Let's get started!' message, an 'Analyze session' button, and a 'Label' dropdown menu.
- Session Info:** A table below the video player providing details about the session.
- Related sessions:** A section on the right side of the session info table, listing other sessions with their dates, times, and statuses.

Session info	
Created	5 days, 18 hours ago
Session ID	51d57b14-c7e4-47fd-8e5c-c098db72ec62
User	[redacted]@delinea.com
Asset	[redacted]
Secret	pra.itp.delinea.app
Secret ID	4
Source	Remote Access
Duration	00:00:03

Related sessions	
05/02/2025 12:10 pm	Recorded
User	[redacted]@delinea.com
Asset	1014.0.5
Duration	00:00:03
04/22/2025 05:02 pm	Analyzed
User	[redacted]@delinea.com
Asset	1014.0.5
Duration	00:00:39
05/02/2025 10:53 am	Recorded
User	[redacted]@delinea.com
Asset	1014.0.5
Duration	00:00:19

Video Controls

The following playback controls are provided when viewing session recordings:

- Full Screen: Display video on your entire window
- Theater Mode: Enable or disable theater viewing mode
- Play/Pause: Play or pause the session
- Previous/Next: Navigate to the previous or next session recording
- Forward/Rewind: Move ahead or rewind the recording in 10 second intervals

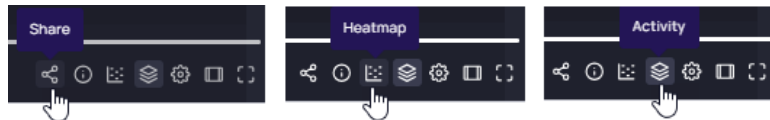
Click the Settings icon in the video tray for Speed controls. To zoom in or out of the video, use the +/- bar provided. Once zoomed, use your mouse to move around the recording. Set the speed for video playback using the predefined selections.

Video Task Bar Features


In addition to the video playback controls, Session Review includes the following features in a task bar embedded in the video player:

Table of Contents


- The Activity icon enables or disables the Activity panel. In the panel, **Analysis with Delinea AI** produces a transcript of activity, including any anomalies identified. See "Analyzing a Recording with AIDA" below
- Click the Heatmap icon to enable or disable detected areas of activity. See "Analyzing a Recording with AIDA" below.
- Click the Share icon to start Session Sharing. You can send a video link to other users on the platform. See "Sharing Sessions" on page 130




Analyzing a Recording with AIDA

 **Note:** This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

With AI-Driven Auditing (AIDA), Session Recording allows you to transcribe the activity in the session video for further analysis. Features include the display of activity as a heatmap and sharing a recording with Delinea Platform users.

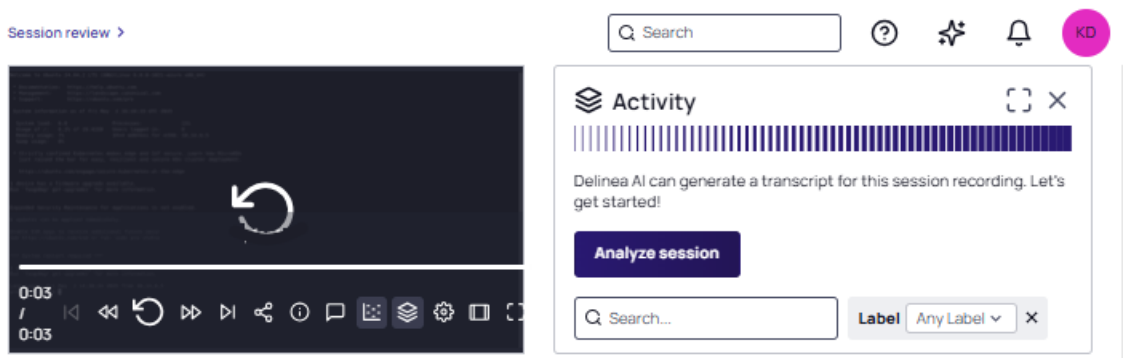
 **Note:** Secret Server Source types are not available for analysis. Analysis is limited to "Privileged Remote Access" on page 290 and "Audit Collector Services" on page 134 source types.

 **Note:** For RDP sessions, AIDA currently analyzes only activity inside PowerShell terminals.

Performing an Analysis

To analyze a session recording:

1. Select a recorded session.
2. Click the Activity icon in the [video player task bar](#) to show the Activity panel if the panel is not displayed.
3. Click **Analyze session**.



The Activity panel is updated with every captured command grouped by activity, with full output, timestamps, and AI-assigned labels.

Table of Contents

A search bar and **Label** filter help you zero in on keywords or behaviors. Use **Autoscroll** to automatically synchronize the video player with the selected activity item. Click either the activity in the Activity panel or a time in the player's timeline to synchronize them.

Q Search

?

☆

🔔

KD

Activity

⌵ ×

Q Search...

Label

Any Label ▾

×

12 items

Note: 5 labels detected

☒ Autoscroll

	TIMESTAMP	ITEM
>	00:00:17	clear
▼	00:00:32	Get-LocalGroupMember
		RecyPS C:\Users\itdradmin > Get-LocalGroupM,
>	00:00:38	ⓘ whoami
>	00:00:52	Test-NetConnection
>	00:01:17	Test-NetConnection
>	00:01:43	Test-NetConnection
>	00:02:03	ⓘ nslookup

🎬

Related sessions

View all →

3 items

05/02/2025 12:10 pm

Analyzed

User

ben.yoder@delinea.com

Asset

20.51.193.57

Duration

00:03:24

Viewing Recording Details

The tabs directly under the video player provide the following details.

Table of Contents

- **Summary** - A concise narrative of the video events. Areas summarized include: Summary of Activities, Critical Errors or Warnings, and Outcome of the Session.
- **Labels** - A roll-up of all labels detected is provided. The same labels are annotated on the [heatmap](#) display in the video taskbar.



Note: Labels are a feature of AIDA () and will appear only if this feature is enabled for your environment.

- **Session Info** - Metadata identifying the video: Created, Session ID, User, Asset, **Secret**, **Secret ID**, **Source**, and **Duration**.
- **Comments** - Comments entered by the user at specific points in the timeline. See "Commenting and Flagging a Session" on the next page.

? ✨ 🔔 KD

Session review >

05/02/2025 12:10 pm Analyzed

Summary

Session info

Comments

Label

Network Operations & Connectivity User & Permission Management

▼ Show more

Summary

Summary of Activities

1. User & Permission Management:

- Executed the command `whoami`, which typically returns the current user's identity, indicating a check on user permissions.

2. Network Operations & Connectivity:

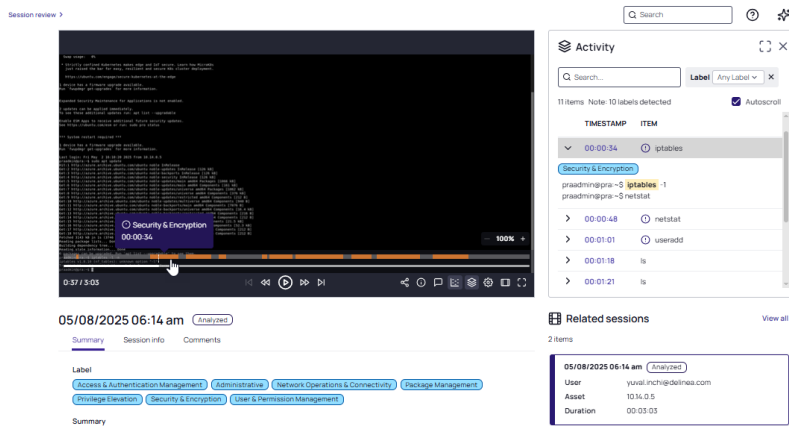
- Multiple instances of `Test-NetConnection` were run to check connectivity to various hosts, including `its.delinea.com` and `google.com`.

Table of Contents

Viewing the Heatmap

After a video is analyzed, click the Heatmap icon in the video player task bar to access a heatmap of the current session.

The heatmap shows an indication of the label identified in the session, along with a short description of the label. Hover over an area of activity to view details. Click an area of the heatmap and the corresponding item in the Activity panel is highlighted.



Commenting and Flagging a Session

In the **Comments** tab, directly under the session recording video player, you can make and view comments. Click the Comment icon in the task bar to view existing comments directly on the time line. Comments are color-coded to individual users.

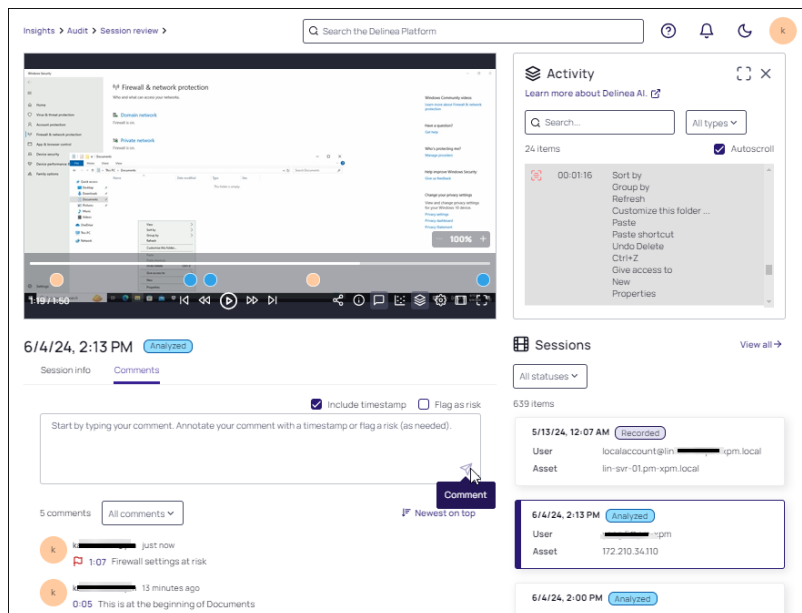



Table of Contents

Enter a comment for the currently selected session directly in the Comment field. Select the **Include timestamp** checkbox to include the time in the saved comment. Select the **Flag as risk** checkbox to include a flag icon in the saved comment.

 **Note:** Comments can only be edited or deleted within five minutes after posting. After that, only replies are available.

Use the dropdown list to choose whether to view all comments or only flagged comments in the list.


Hover over any comment to view the **Reply** link and enter a reply.



Sharing Sessions

You can share recordings within the platform with other users, as long as all users have the same session recording permissions. See "Roles and Permissions" on page 203.

1. In the Session review page, select the recording you want to share.

 **Note:** You can also select a specific time in the video where playback will begin.

2. In the [video player controls](#), click the Share icon.
3. In the Share a link dialog, click the copy icon.
4. Use your preferred method (for example, email or messaging app) to send another user the link you just copied.



Reviewing Audit Logs

Audit logs are used to communicate monitored activity occurring across the platform.

Accessing Audit Logs

To access Audit logs:

Table of Contents

1. Go to the Delinea Platform home page.
2. From the left panel, click **Insights**, then click **Audit logs**.

Viewing The Audit Log

Events that your account has permissions to view are presented in the Audit logs table. Click any row in the table to view its **Event details** in the review panel.

The **Action** column of the log captures user behavior and may include hyperlinks to additional properties.

DATE ↓	SERVICE	LEVEL	ACTION
12/16/24, 1:02 PM	Identity	Privileged Activity	Multi-factor authentication attempted by kate@delinea.com .
12/16/24, 1:02 PM	Identity	Security Audit	Login for user kate@delinea.com started.
12/16/24, 1:02 PM	Secret Server	Privileged Activity	Secret 136 file was saved by delineaidservice .
12/16/24, 1:00 PM	Secret Server	Privileged Activity	Secret 137 was viewed by delineaidservice .
12/16/24, 1:00 PM	Secret Server	Privileged Activity	Secret 136 was viewed by delineaidservice .
12/16/24, 12:56 PM	Identity	Privileged Activity	kate@delinea.com successfully logged out.
12/16/24, 12:56 PM	Identity	Security Audit	Authenticated session for user kate@delinea.com .
12/16/24, 12:52 PM	Secret Server	Privileged Activity	Secret 136 file was saved by delineaidservice .

Customizing the Audit Log Table

The columns in the Audit Log table present data associated with the event. Some columns can be sorted in either ascending or descending order. You can customize which columns are presented using the Displayed Columns icon (≡).

The columns are:

Column	Definition
Date	The time stamp when the audit event occurred
Service	The platform service where the audit event took place (e.g., Secret Server, Inventory, etc.) For a description of the services available for monitoring, see "Selecting Audit Levels for Display" on the next page.

Table of Contents

Level	The classification of the audit event (Security Audit or Privilege Activity) For a description of the levels available for monitoring, see "Selecting Audit Levels for Display" below.
Event Type	The category of action performed, such as Secret View, Secret Checkout, or Alert Created.
Action	The behavior that produced the event
Initiated By	The username of the platform user who triggered the audit event
Target	The specific entity affected by the audit event, such as a secret
Source	The specific source affected by the audit event (e.g., machine host name, IP address, etc.)
Field Changes	The changes made to any field for each action logged

Filtering Events

By default, the last 7 days of events are shown. Other options include 24 hours, 48 hours, 3 days, 7 days, 30 days, or 60 days. To change the time period, use the dropdown list in the **Date** filter card.

To further narrow down the list of events, click **Add filter**. Select the desired filter criteria. Its associated card appears at the top of the table. Use the card's dropdown list to set the desired value for filtering. For more information, see ["Filtering in List Pages"](#) on page 48.

Selecting Audit Levels for Display

The event logs are divided into two categories:

- **Security Audit** logs include critical actions, such as configuration changes in Delinea services.
- **Privileged Activity** logs include actions that are important, but not critical, such as creating secrets, viewing passwords, or launching an elevated process on an endpoint.

To choose which category to display, click **Add filter** and select the **Level** filter criteria. Use the **Level** dropdown list to indicate the categories to display. (For more information about filtering, see ["Filtering in List Pages"](#) on page 48.)

Table of Contents

Insights >

Q Search



Audit logs ☆ 🔗

Q Search...	Date Last 7 days ▾	Service Any Service ▾ X	Type Any Type ▾ X	Level Privileged Activity ▾ X
🔍 Add filter				1 Selected Clear all
3,224 items				<input type="checkbox"/> Security Audit
				<input checked="" type="checkbox"/> Privileged Activity
DATE ↓	SERVICE	LEVEL	ACTION	
12/16/24, 1:18 PM	Identity	Privileged Activity	Multi-factor authentication attempted by yanagisawa.yoshiaki .	
12/16/24, 1:12 PM	Secret Server	Privileged Activity	Secret 136 file was saved by delineaitdrservice .	
12/16/24, 1:12 PM	Secret Server	Privileged Activity	Secret 136 was viewed by delineaitdrservice .	
12/16/24, 1:02 PM	Identity	Privileged Activity	Multi-factor authentication attempted by yanagisawa.yoshiaki .	
12/16/24, 1:02 PM	Secret Server	Privileged Activity	Secret 136 file was saved by delineaitdrservice .	
12/16/24, 1:00 PM	Secret Server	Privileged Activity	Secret 137 was viewed by delineaitdrservice .	
12/16/24, 1:00 PM	Secret Server	Privileged Activity	Secret 136 was viewed by delineaitdrservice .	

For a detailed list of the Services that support these levels, see the following:

- "Audit Collector Services" on the next page
- "Engine Management Services" on page 148
- "Identity Services" on page 148
- "Identity Federation Services" on page 150
- "MFA Providers Services" on page 151
- "Permissions Services" on page 152
- "Policy Services" on page 152
- "Privileged Remote Access Services" on page 153
- "Registration Services" on page 154
- "Secret Server Services" on page 154
- "Session Recording Services" on page 161
- "Tenant Profile Services" on page 161

Downloading Event Log Data

The data from the event log can be downloaded as a CSV file.

1. Click the Download icon in the top control bar.
2. In the Download dialog, specify a **File Name**.
3. In **Data Format**, choose a **User Format** or **ISO** format as the format for the CSV file label.
4. Click **Download**.

Table of Contents

Download

Download CSV

Records 30

File Name event-log.csv

Date Format ISO (2022-12-07T13:40:27.101Z)
User Format (12/07/2022 08:40 am)

Cancel Download

Audit Collector Services

- Privilege run failed by user {{Actor.Name}}.
- User {{Actor.Name}} successfully logged in via the console.
- Console Login attempt by user {{Actor.Name}} failed.
- User {{Actor.Name}} successfully logged in remotely.
- Remote Login attempt by user {{Actor.Name}} failed.
- Desktop creation failed by user {{Actor.Name}}.
- Self-service account unlock attempt failed by user {{Actor.Name}}.
- Run with privilege as an alternate user failed by user {{Actor.Name}}.
- Run with an alternate account failed by user {{Actor.Name}}.
- MFA challenge was failed by user {{Actor.Name}}.
- MFA challenge was failed by user {{Actor.Name}}.
- MFA challenge was failed by user {{Actor.Name}}.
- Setting up offline MFA profile failed by user {{Actor.Name}}.
- MFA challenge was failed by user {{Actor.Name}}.
- PowerShell remote command was executed by user {{Actor.Name}}.
- Windows authentication was skipped by user {{Actor.Name}}.
- Setting up offline MFA profile succeeded for user {{Actor.Name}}.
- Self-service password reset attempt failed by user {{Actor.Name}}.
- Self-service account unlock was successful for user {{Actor.Name}}.
- Privilege run succeeded by user {{Actor.Name}}.
- Running with privilege as an alternate user succeeded by user {{Actor.Name}}.
- Run with an alternate account was successful by user {{Actor.Name}}.

Table of Contents

- PowerShell remote connection was successful for user {{Actor.Name}}.
- Network access was successful for user {{Actor.Name}}.
- MFA was skipped by user {{Actor.Name}}.
- MFA challenge was successful for user {{Actor.Name}}.
- MFA challenge was successful for user {{Actor.Name}}.
- MFA challenge was successful for user {{Actor.Name}}.
- MFA challenge was successful for user {{Actor.Name}}.
- Successful departure from the zone by user {{Actor.Name}}.
- Joining the zone was successful for user {{Actor.Name}}.
- Desktop creation was successful for user {{Actor.Name}}.
- User {{Actor.Name}} changed their password.
- Monitoring of command execution started by user {{Actor.Name}}.
- Monitored command execution failed by user {{Actor.Name}}.
- dzsshchk was granted to user {{Actor.Name}}.
- dzsshchk was denied to user {{Actor.Name}}.
- sshd was granted to user {{Actor.Name}}.
- sshd was denied to user {{Actor.Name}}.
- sshd was granted to user {{Actor.Name}}.
- sshd was denied to user {{Actor.Name}}.
- scp execution succeeded for user {{Actor.Name}}.
- scp execution failed for user {{Actor.Name}}.
- sftp command execution was successful for user {{Actor.Name}}.
- sftp command execution failed by user {{Actor.Name}}.
- PAM authentication was granted to user {{Actor.Name}}.
- PAM authentication was denied to user {{Actor.Name}}.
- PAM authentication was granted to user {{Actor.Name}}.
- PAM authentication was denied to user {{Actor.Name}}.
- PAM set credentials were granted to user {{Actor.Name}}.
- PAM set credentials were denied to user {{Actor.Name}}.
- PAM account management was granted to user {{Actor.Name}}.
- PAM account management was denied to user {{Actor.Name}}.
- PAM change authentication token was granted to user {{Actor.Name}}.
- PAM change authentication token was denied to user {{Actor.Name}}.

Table of Contents

- PAM open session was granted to user {{Actor.Name}}.
- PAM open session was denied to user {{Actor.Name}}.
- PAM close session was granted to user {{Actor.Name}}.
- PAM close session was denied to user {{Actor.Name}}.
- PAM rescue mode succeeded for user {{Actor.Name}}.
- dzdo was granted to user {{Actor.Name}}.
- dzdo was denied to user {{Actor.Name}}.
- dzdo ticket was successful for user {{Actor.Name}}.
- dzdo was granted to user {{Actor.Name}}.
- dzdo was denied to user {{Actor.Name}}.
- dzdo started command execution for user {{Actor.Name}}.
- dzdo ended command execution for user {{Actor.Name}}.
- dzsh was granted to user {{Actor.Name}}.
- dzsh was denied to user {{Actor.Name}}.
- dzsh was granted to user {{Actor.Name}}.
- dzsh was denied to user {{Actor.Name}}.
- dzsh role change was granted to user {{Actor.Name}}.
- dzsh role change was denied to user {{Actor.Name}}.
- Enabling Identity Services Platform failed for user {{Actor.Name}}.
- Disabling Identity Services Platform failed for user {{Actor.Name}}.
- Local user was enabled by user {{Actor.Name}}.
- Identity Services Platform was successfully enabled by user {{Actor.Name}}.
- Local user was disabled by user {{Actor.Name}}.
- Identity Services Platform was successfully disabled by user {{Actor.Name}}.
- Role was successfully added by user {{Actor.Name}}.
- Role assignment was successfully added by user {{Actor.Name}}.
- Session was deleted by selection by user {{Actor.Name}}.
- Session was deleted by query by user {{Actor.Name}}.
- Session reviewers were set successfully by user {{Actor.Name}}.
- Session reviewers were removed successfully by user {{Actor.Name}}.
- Session review status was updated successfully by user {{Actor.Name}}.
- Session replay succeeded by user {{Actor.Name}}.
- Audit events were deleted successfully by user {{Actor.Name}}.

Table of Contents

- Deleting audit events failed for user {{Actor.Name}}.
- Session was deleted successfully by user {{Actor.Name}}.
- Deleting session failed for user {{Actor.Name}}.
- Video Auditing was configured by user {{Actor.Name}}.
- Installation was created successfully by user {{Actor.Name}}.
- Creating installation failed for user {{Actor.Name}}.
- Installation was updated successfully by user {{Actor.Name}}.
- Updating installation failed for user {{Actor.Name}}.
- Installation permissions were updated successfully by user {{Actor.Name}}.
- Updating installation permissions failed for user {{Actor.Name}}.
- Installation was removed successfully by user {{Actor.Name}}.
- Removing installation failed for user {{Actor.Name}}.
- Management Database was added successfully by user {{Actor.Name}}.
- Adding Management Database failed for user {{Actor.Name}}.
- Management Database was updated successfully by user {{Actor.Name}}.
- Updating Management Database failed for user {{Actor.Name}}.
- Management Database permissions were updated successfully by user {{Actor.Name}}.
- Updating Management Database permissions failed for user {{Actor.Name}}.
- Management Database was removed successfully by user {{Actor.Name}}.
- Removing Management Database failed for user {{Actor.Name}}.
- Audit Store was added successfully by user {{Actor.Name}}.
- Adding Audit Store failed for user {{Actor.Name}}.
- Audit Store was updated successfully by user {{Actor.Name}}.
- Updating Audit Store failed for user {{Actor.Name}}.
- Audit Store permissions were updated successfully by user {{Actor.Name}}.
- Updating Audit Store permissions failed for user {{Actor.Name}}.
- Audit Store was removed successfully by user {{Actor.Name}}.
- Removing Audit Store failed for user {{Actor.Name}}.
- Audit Store Database was added successfully by user {{Actor.Name}}.
- Adding Audit Store Database failed for user {{Actor.Name}}.
- Audit Store Database was attached successfully by user {{Actor.Name}}.
- Attaching Audit Store Database failed for user {{Actor.Name}}.
- Audit Store Database was attached successfully by user {{Actor.Name}}.

Table of Contents

- Attaching Audit Store Database failed for user {{Actor.Name}}.
- Active Audit Store Database was set successfully by user {{Actor.Name}}.
- Setting active Audit Store Database failed for user {{Actor.Name}}.
- Audit Store Database was updated successfully by user {{Actor.Name}}.
- Updating Audit Store Database failed for user {{Actor.Name}}.
- Audit Store Database was detached successfully by user {{Actor.Name}}.
- Detaching Audit Store Database failed for user {{Actor.Name}}.
- Audit Store Database was deleted successfully by user {{Actor.Name}}.
- Deleting Audit Store Database failed for user {{Actor.Name}}.
- Audit Role was added successfully by user {{Actor.Name}}.
- Adding Audit Role failed for user {{Actor.Name}}.
- Audit Role was updated successfully by user {{Actor.Name}}.
- Updating Audit Role failed for user {{Actor.Name}}.
- Audit Role permissions were updated successfully by user {{Actor.Name}}.
- Updating Audit Role permissions failed for user {{Actor.Name}}.
- Audit Role Member was assigned successfully by user {{Actor.Name}}.
- Assigning Audit Role Member failed for user {{Actor.Name}}.
- Audit Role Member was removed successfully by user {{Actor.Name}}.
- Removing Audit Role Member failed for user {{Actor.Name}}.
- Audit Role was deleted successfully by user {{Actor.Name}}.
- Deleting Audit Role failed for user {{Actor.Name}}.
- Audit Compliance Policy was configured by user {{Actor.Name}}.
- License Key was added successfully by user {{Actor.Name}}.
- Adding License Key failed for user {{Actor.Name}}.
- License Key was removed successfully by user {{Actor.Name}}.
- Removing License Key failed for user {{Actor.Name}}.
- DA Enable was granted by user {{Actor.Name}}.
- DA Enable was denied by user {{Actor.Name}}.
- DA Disable was granted by user {{Actor.Name}}.
- DA Disable was denied by user {{Actor.Name}}.
- Desktop auditing was enabled by user {{Actor.Name}}.
- Desktop auditing enable was denied by user {{Actor.Name}}.
- Desktop auditing was disabled by user {{Actor.Name}}.

Table of Contents

- Desktop auditing disable was denied by user {{Actor.Name}}.
- adpasswd command succeeded for user {{Actor.Name}}.
- adpasswd command failed for user {{Actor.Name}}.
- Monitor was enabled by user {{Actor.Name}}.
- Monitor enable was denied by user {{Actor.Name}}.
- Monitor was disabled by user {{Actor.Name}}.
- Monitor disable was denied by user {{Actor.Name}}.
- adwebproxyconf command succeeded for user {{Actor.Name}}.
- adwebproxyconf command failed for user {{Actor.Name}}.
- adkeytab command succeeded for user {{Actor.Name}}.
- adkeytab command failed for user {{Actor.Name}}.
- Enabled local user was added successfully by user {{Actor.Name}}.
- Updating local passwd file failed for user {{Actor.Name}}.
- Disabled local user was added successfully by user {{Actor.Name}}.
- Local user was removed successfully by user {{Actor.Name}}.
- Local user was disabled successfully by user {{Actor.Name}}.
- Local user was enabled successfully by user {{Actor.Name}}.
- Enabled local group was added successfully by user {{Actor.Name}}.
- Updating local group file failed for user {{Actor.Name}}.
- Local group was removed successfully by user {{Actor.Name}}.
- admanagelocal command succeeded for user {{Actor.Name}}.
- admanagelocal command failed for user {{Actor.Name}}.
- Trusted path was granted to user {{Actor.Name}}.
- Trusted path was denied to user {{Actor.Name}}.
- Zone administrative tasks were delegated by user {{Actor.Name}}.
- Delegation of zone administrative tasks failed by user {{Actor.Name}}.
- Computer administrative tasks were delegated by user {{Actor.Name}}.
- Delegation of computer administrative tasks failed by user {{Actor.Name}}.
- Computer role administrative tasks were delegated by user {{Actor.Name}}.
- Delegation of computer role administrative tasks failed by user {{Actor.Name}}.
- Zone was created by user {{Actor.Name}}.
- Zone creation failed by user {{Actor.Name}}.
- Zone was deleted by user {{Actor.Name}}.

Table of Contents

- Zone deletion failed by user {{Actor.Name}}.
- Zone was modified by user {{Actor.Name}}.
- Zone update failed by user {{Actor.Name}}.
- User was added to a zone by user {{Actor.Name}}.
- Adding user to a zone failed by user {{Actor.Name}}.
- User was deleted from a zone by user {{Actor.Name}}.
- Deleting user from a zone failed by user {{Actor.Name}}.
- User profile in a zone was modified by user {{Actor.Name}}.
- Modifying user in a zone failed by user {{Actor.Name}}.
- User was added to a computer by user {{Actor.Name}}.
- Adding user to a computer failed by user {{Actor.Name}}.
- User was deleted from a computer by user {{Actor.Name}}.
- Deleting user from a computer failed by user {{Actor.Name}}.
- User profile on a computer was modified by user {{Actor.Name}}.
- Modifying user on a computer failed by user {{Actor.Name}}.
- Group was added to a zone by user {{Actor.Name}}.
- Adding group to a zone failed by user {{Actor.Name}}.
- Group was deleted from a zone by user {{Actor.Name}}.
- Deleting group from a zone failed by user {{Actor.Name}}.
- Group profile in a zone was modified by user {{Actor.Name}}.
- Modifying group in a zone failed by user {{Actor.Name}}.
- Group was added to a computer by user {{Actor.Name}}.
- Adding group to a computer failed by user {{Actor.Name}}.
- Group was deleted from a computer by user {{Actor.Name}}.
- Deleting group from a computer failed by user {{Actor.Name}}.
- Group profile on a computer was modified by user {{Actor.Name}}.
- Modifying group on a computer failed by user {{Actor.Name}}.
- Computer was added by user {{Actor.Name}}.
- Adding computer failed by user {{Actor.Name}}.
- Computer was deleted by user {{Actor.Name}}.
- Deleting computer failed by user {{Actor.Name}}.
- Computer was modified by user {{Actor.Name}}.
- Modifying computer failed by user {{Actor.Name}}.

Table of Contents

- PAM access right was added by user {{Actor.Name}}.
- Adding PAM right failed by user {{Actor.Name}}.
- PAM right was deleted by user {{Actor.Name}}.
- Deleting PAM right failed by user {{Actor.Name}}.
- PAM right was modified by user {{Actor.Name}}.
- Modifying PAM right failed by user {{Actor.Name}}.
- UNIX command right was added by user {{Actor.Name}}.
- Adding UNIX command right failed by user {{Actor.Name}}.
- UNIX command right was deleted by user {{Actor.Name}}.
- Deleting UNIX command right failed by user {{Actor.Name}}.
- UNIX command right was modified by user {{Actor.Name}}.
- Modifying UNIX command right failed by user {{Actor.Name}}.
- Role was added by user {{Actor.Name}}.
- Adding role failed by user {{Actor.Name}}.
- Role was deleted by user {{Actor.Name}}.
- Deleting role failed by user {{Actor.Name}}.
- Role was modified by user {{Actor.Name}}.
- Modifying role failed by user {{Actor.Name}}.
- Right was successfully added to a role by user {{Actor.Name}}.
- Adding right to a role failed by user {{Actor.Name}}.
- Right was successfully deleted from a role by user {{Actor.Name}}.
- Deleting right from a role failed by user {{Actor.Name}}.
- Role assignment was added by user {{Actor.Name}}.
- Adding role assignment failed by user {{Actor.Name}}.
- Role assignment was removed by user {{Actor.Name}}.
- Deleting role assignment failed by user {{Actor.Name}}.
- Role assignment was modified by user {{Actor.Name}}.
- Modifying role assignment failed by user {{Actor.Name}}.
- Role assignment was added to a computer by user {{Actor.Name}}.
- Adding role assignment to a computer failed by user {{Actor.Name}}.
- Role assignment was deleted from a computer by user {{Actor.Name}}.
- Deleting role assignment from a computer failed by user {{Actor.Name}}.
- Role assignment was modified for a computer by user {{Actor.Name}}.

Table of Contents

- Modifying role assignment for a computer failed by user {{Actor.Name}}.
- Role assignment was added to a computer role by user {{Actor.Name}}.
- Adding role assignment to a computer role failed by user {{Actor.Name}}.
- Role assignment was deleted from a computer role by user {{Actor.Name}}.
- Deleting role assignment from a computer role failed by user {{Actor.Name}}.
- Role assignment for a computer role was modified by user {{Actor.Name}}.
- Modifying role assignment in a computer role failed by user {{Actor.Name}}.
- Computer role was added by {{Actor.Name}}.
- Adding computer role failed by {{Actor.Name}}.
- Computer role was deleted by {{Actor.Name}}.
- Deleting computer role failed by {{Actor.Name}}.
- Computer role was modified by {{Actor.Name}}.
- Modifying computer role failed by {{Actor.Name}}.
- User was added to a group by {{Actor.Name}}.
- Adding user to a group failed by {{Actor.Name}}.
- Password was reset by {{Actor.Name}}.
- Resetting password failed by {{Actor.Name}}.
- Desktop right was added by {{Actor.Name}}.
- Adding desktop right failed by {{Actor.Name}}.
- Desktop right was deleted by {{Actor.Name}}.
- Deleting desktop right failed by {{Actor.Name}}.
- Desktop right was modified by {{Actor.Name}}.
- Modifying desktop right failed by {{Actor.Name}}.
- Network right was added by {{Actor.Name}}.
- Adding network right failed by {{Actor.Name}}.
- Network right was deleted by {{Actor.Name}}.
- Deleting network right failed by {{Actor.Name}}.
- Network right was modified by {{Actor.Name}}.
- Modifying network right failed by {{Actor.Name}}.
- Application right was added by {{Actor.Name}}.
- Adding application right failed by {{Actor.Name}}.
- Application right was deleted by {{Actor.Name}}.
- Deleting application right failed by {{Actor.Name}}.

Table of Contents

- Application right was modified by {{Actor.Name}}.
- Modifying application right failed by {{Actor.Name}}.
- Local user was added to a zone by {{Actor.Name}}.
- Adding local user to a zone failed by {{Actor.Name}}.
- Local user was deleted from a zone by {{Actor.Name}}.
- Deleting local user from a zone failed by {{Actor.Name}}.
- Local user profile in a zone was modified by {{Actor.Name}}.
- Modifying local user in a zone failed by {{Actor.Name}}.
- Local user was added to a computer by {{Actor.Name}}.
- Adding local user to a computer failed by {{Actor.Name}}.
- Local user was deleted from a computer by {{Actor.Name}}.
- Deleting local user from a computer failed by {{Actor.Name}}.
- Local user profile on a computer was modified by {{Actor.Name}}.
- Modifying local user on a computer failed by {{Actor.Name}}.
- Local group was added to a zone by {{Actor.Name}}.
- Adding local group to a zone failed by {{Actor.Name}}.
- Local group was deleted from a zone by {{Actor.Name}}.
- Deleting local group from a zone failed by {{Actor.Name}}.
- Local group profile in a zone was modified by {{Actor.Name}}.
- Modifying local group in a zone failed by {{Actor.Name}}.
- Local group was added to a computer by {{Actor.Name}}.
- Adding local group to a computer failed by {{Actor.Name}}.
- Local group was deleted from a computer by {{Actor.Name}}.
- Deleting local group from a computer failed by {{Actor.Name}}.
- Local group profile on a computer was modified by {{Actor.Name}}.
- Modifying local group for a computer failed by {{Actor.Name}}.
- Local Windows user was added to a zone by {{Actor.Name}}.
- Adding local Windows user to a zone failed by {{Actor.Name}}.
- Local Windows user was deleted from a zone by {{Actor.Name}}.
- Deleting local Windows user from a zone failed by {{Actor.Name}}.
- Local Windows user in a zone was modified by {{Actor.Name}}.
- Modifying local Windows user in a zone failed by {{Actor.Name}}.
- Local Windows user was added to a computer by {{Actor.Name}}.

Table of Contents

- Adding local Windows user to a computer failed by {{Actor.Name}}.
- Local Windows user was deleted from a computer by {{Actor.Name}}.
- Deleting local Windows user from a computer failed by {{Actor.Name}}.
- Local Windows user on a computer was modified by {{Actor.Name}}.
- Modifying local Windows user on a computer failed by {{Actor.Name}}.
- Local Windows group was added to a zone by {{Actor.Name}}.
- Adding local Windows group to a zone failed by {{Actor.Name}}.
- Local Windows group was deleted from a zone by {{Actor.Name}}.
- Deleting local Windows group from a zone failed by {{Actor.Name}}.
- Local Windows group in a zone was modified by {{Actor.Name}}.
- Modifying local Windows group in a zone failed by {{Actor.Name}}.
- Local Windows group was added to a computer by {{Actor.Name}}.
- Adding local Windows group to a computer failed by {{Actor.Name}}.
- Local Windows group was deleted from a computer by {{Actor.Name}}.
- Deleting local Windows group from a computer failed by {{Actor.Name}}.
- Local Windows group on a computer was modified by {{Actor.Name}}.
- Modifying local Windows group for a computer failed by {{Actor.Name}}.
- {{Actor.Name}} failed to create the zone.
- {{Actor.Name}} encountered an error while attempting to leave the zone.
- {{Actor.Name}} failed to add a new role.
- {{Actor.Name}} experienced a failure while trying to assign a role.
- {{Actor.Name}}'s attempt to switch the desktop was unsuccessful.
- {{Actor.Name}} faced a login error in PowerShell.
- {{Actor.Name}} encountered an error while starting the collector.
- {{Actor.Name}} failed to stop the collector.
- {{Actor.Name}} experienced a failure while updating the collector's settings.
- The agent failed to start for {{Actor.Name}}.
- {{Actor.Name}} encountered an issue while stopping the agent.
- {{Actor.Name}} failed to update the agent's settings.
- Starting the AuditManager was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} failed to stop the AuditManager.
- {{Actor.Name}} experienced a failure while trying to start the collector.
- The collector failed to stop for {{Actor.Name}}.

Table of Contents

- {{Actor.Name}} failed to restart the collector.
- {{Actor.Name}} experienced a failure while attempting to start the AuditManager.
- Stopping the AuditManager was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} failed to restart the AuditManager.
- {{Actor.Name}}'s attempt to add a local user failed.
- {{Actor.Name}} failed to remove the local user.
- {{Actor.Name}} failed to enable the local user.
- {{Actor.Name}} failed to disable the local user.
- Modifying the local user was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} faced an error while adding a local group.
- {{Actor.Name}} failed to remove the local group.
- {{Actor.Name}} experienced a problem while modifying the local group.
- {{Actor.Name}} failed to manage local accounts.
- {{Actor.Name}} failed to invoke the command through the notification.
- {{Actor.Name}} successfully entered the ticket.
- {{Actor.Name}} successfully switched desktop.
- {{Actor.Name}} successfully stopped the collector.
- {{Actor.Name}} successfully stopped the collector.
- {{Actor.Name}} successfully stopped the AuditManager.
- Stopping the AuditManager was successful for {{Actor.Name}}.
- {{Actor.Name}} was successful in stopping the agent.
- {{Actor.Name}} successfully started the collector.
- Starting the collector was a success for {{Actor.Name}}.
- {{Actor.Name}} started the AuditManager successfully.
- {{Actor.Name}} successfully initiated the AuditManager.
- The agent started successfully for {{Actor.Name}}.
- {{Actor.Name}} initiated Windows session auditing.
- {{Actor.Name}} ended the Windows session auditing.
- {{Actor.Name}} restarted the collector successfully.
- Restarting the AuditManager was successful for {{Actor.Name}}.
- {{Actor.Name}} successfully removed the local user.
- {{Actor.Name}} successfully removed local group.
- {{Actor.Name}} successfully modified local user.

Table of Contents

- {{Actor.Name}} successful modified local group.
- Multi-factor authentication (MFA) went offline for {{Actor.Name}}.
- {{Actor.Name}} successfully managed local accounts.
- {{Actor.Name}} successfully invoked a command through the notification.
- {{Actor.Name}} successfully updated the collector's settings.
- The agent's settings were successfully updated by {{Actor.Name}}.
- {{Actor.Name}} successfully added a new local group.
- {{Actor.Name}} successfully added an enabled local user.
- {{Actor.Name}} successfully added a disabled local user.
- {{Actor.Name}} faced an error while setting session reviewers.
- {{Actor.Name}} failed to remove session reviewers.
- {{Actor.Name}} failed to update the review status of the session.
- {{Actor.Name}} experienced a failure during the session replay.
- File monitoring was initiated by {{Actor.Name}}.
- File monitoring failed for {{Actor.Name}}.
- {{Actor.Name}} began executing a command.
- Command execution failed for {{Actor.Name}}.
- The AD Client started successfully for {{Actor.Name}}.
- Starting the AD Client was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} successfully stopped the AD Client.
- {{Actor.Name}} failed to stop the AD Client.
- {{Actor.Name}} initiated advanced monitoring command execution.
- Advanced monitoring command execution failed for {{Actor.Name}}.
- Advanced file monitoring was started by {{Actor.Name}}.
- {{Actor.Name}} experienced a failure with advanced file monitoring.
- {{Actor.Name}} started monitoring command history successfully.
- Monitoring command history failed for {{Actor.Name}}.
- {{Actor.Name}} successfully started the daemon.
- Daemon start-up was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} successfully stopped the daemon.
- {{Actor.Name}} faced an error while stopping the daemon.
- {{Actor.Name}} successfully executed the Delinea CDash command.
- Unix session auditing was initiated by {{Actor.Name}}.

Table of Contents

- {{Actor.Name}} ended the Unix session auditing.
- {{Actor.Name}} successfully joined AD using Delinea commands.
- {{Actor.Name}} failed to join AD using Delinea commands.
- {{Actor.Name}} left AD successfully using Delinea commands.
- {{Actor.Name}} experienced a failure while leaving AD with Delinea commands.
- {{Actor.Name}} successfully executed the Delinea AD query root command.
- {{Actor.Name}} successfully queried a user in AD using Delinea commands.
- {{Actor.Name}} faced an error while querying AD with Delinea commands.
- The AD reload was successfully executed by {{Actor.Name}} using Delinea commands.
- {{Actor.Name}} failed to reload AD using Delinea commands.
- {{Actor.Name}} successfully flushed AD using Delinea commands.
- AD flush was unsuccessful for {{Actor.Name}} using Delinea commands.
- {{Actor.Name}} successfully refreshed AD objects using Delinea commands.
- Delinea AD object refresh failed for {{Actor.Name}}.
- {{Actor.Name}} successfully executed the Delinea AD license command.
- The Delinea AD license command failed for {{Actor.Name}}.
- {{Actor.Name}} successfully closed the SSHD connection.
- The audited command was successfully executed by {{Actor.Name}}.
- The execution of the audited command failed for {{Actor.Name}}.
- {{Actor.Name}} generated the Kerberos credential cache name successfully.
- Kerberos credential cache name generation failed for {{Actor.Name}}.
- {{Actor.Name}} initialized the Kerberos credential cache successfully.
- Initialization of the Kerberos credential cache failed for {{Actor.Name}}.
- {{Actor.Name}} destroyed the Kerberos credential cache successfully.
- {{Actor.Name}} failed to destroy the Kerberos credential cache.
- {{Actor.Name}} updated the Kerberos credential cache successfully.
- Updating the Kerberos credential cache was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} successfully retrieved the credentials in the given Kerberos cache.
- Retrieving credentials in the given Kerberos cache failed for {{Actor.Name}}.
- {{Actor.Name}} read the principal in the given Kerberos cache successfully.
- Reading the principal in the given Kerberos cache failed for {{Actor.Name}}.
- {{Actor.Name}} iterated through the credentials in the given Kerberos cache successfully.
- Iterating through the credentials in the given Kerberos cache failed for {{Actor.Name}}.

Table of Contents

- {{Actor.Name}} read the credentials in the given Kerberos cache successfully.
- Reading credentials in the given Kerberos cache was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} removed credentials from the Kerberos cache successfully.
- Removing credentials from the Kerberos cache failed for {{Actor.Name}}.
- {{Actor.Name}} successfully iterated through the Kerberos credential cache.
- Iterating the Kerberos credential cache was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} read the Kerberos credential cache successfully.
- Reading the Kerberos credential cache failed for {{Actor.Name}}.
- {{Actor.Name}} changed the ownership for the given Kerberos credential cache successfully.
- Changing ownership for the given Kerberos credential cache failed for {{Actor.Name}}.
- {{Actor.Name}} read the status for the given Kerberos credential cache successfully.
- Reading the status for the given Kerberos credential cache failed for {{Actor.Name}}.
- {{Actor.Name}} successfully invoked the notification CLI for the local account.
- Invoking the notification CLI for the local account was unsuccessful for {{Actor.Name}}.
- {{Actor.Name}} successfully logged in using Multi-Factor Authentication (MFA).
- {{Actor.Name}} failed to log in using Multi-Factor Authentication (MFA).
- {{Actor.Name}} successfully logged in using Multi-Factor Authentication (MFA).
- {{Actor.Name}} failed to log in using Multi-Factor Authentication (MFA).
- {{Actor.Name}} successfully retrieved information using the Dzinfo command.
- {{Actor.Name}} faced an error while trying to retrieve information using the Dzinfo command.

Engine Management Services

- Site {{Target.Name}} was modified by user {{Actor.Name}}.
- Site {{Target.Name}} was deleted by user {{Actor.Name}}.
- Engine {{Target.Name}} was created by user {{Actor.Name}}.
- Engine {{Target.Name}} was modified by user {{Actor.Name}}.
- Engine {{Target.Name}} was deleted by user {{Actor.Name}}.
- Engine upgrade(s) requested by user {{Actor.Name}}: {{AdditionalAttributes.EngineIds | join: ", "}}
- Engine {{Target.Name}} capabilities updated by user {{Actor.Name}}. Current capabilities {{AdditionalAttributes.Groups | join: ", "}}.

Identity Services

- Authenticated session for user {{Actor.Name}} started.
- Authenticated session for user {{Actor.Name}} upgraded.

Table of Contents

- Authenticated session for user {{Actor.Name}} ended.
- Rights check failure occurred for {{Actor.Name}}.
- Access rights event was triggered.
- Access point was created by {{Actor.Name}}.
- Access was removed by {{Actor.Name}}.
- Role-based access event was triggered by {{Actor.Name}}.
- Access point was edited by {{Actor.Name}}.
- Admin MFA security question was added by {{Actor.Name}}.
- Admin MFA security question was deleted by {{Actor.Name}}.
- MFA profile was created by {{Actor.Name}}.
- MFA AuthProfile was deleted by {{Actor.Name}}.
- MFA profile was updated by {{Actor.Name}}.
- Auth Session was upgraded by {{Actor.Name}}.
- MFA challenge definition was created by {{Actor.Name}}.
- MFA Challenge was deleted by {{Actor.Name}}.
- MFA challenge definition was updated by {{Actor.Name}}.
- Custom user was created by {{Actor.Name}}.
- Custom user in Directory Services was deleted by {{Actor.Name}}.
- Custom user was updated by {{Actor.Name}}.
- User state was set by {{Actor.Name}}.
- Admin account password was updated by {{Actor.Name}}.
- Password change in Directory Services failed due to {{Actor.Name}}.
- Custom policy was created by {{Actor.Name}}.
- DS entity was changed by {{Actor.Name}}
- Directory service was removed by {{Actor.Name}}
- Extended column was added by {{Actor.Name}}
- Extended column was removed by {{Actor.Name}}
- Directory was deleted by {{Actor.Name}}
- File was deleted by {{Actor.Name}}
- Username was forgotten by {{Actor.Name}}.
- Directory group was created by {{Actor.Name}}.
- Group in Directory Services was deleted by {{Actor.Name}}.
- {{Actor.Name}} successfully logged out.

Table of Contents

- Multi-factor authentication summary was viewed by {{Actor.Name}}.
- MFA was challenged for {{Actor.Name}}.
- {{Actor.Name}} responded to the MFA challenge.
- OATH token was confirmed by {{Actor.Name}}.
- OATH token was resynced by {{Actor.Name}}.
- OATH token resync failed for {{Actor.Name}}.
- Invalid client was detected by {{Actor.Name}}.
- Invalid client credentials were detected by {{Actor.Name}}.
- Policy set was created by {{Actor.Name}}.
- Policy set was deleted by {{Actor.Name}}.
- Policy set was updated by {{Actor.Name}}.
- The Plink policy was changed by {{Actor.Name}}.
- Plink order policy was changed by {{Actor.Name}}.
- Policy configuration was updated by {{Actor.Name}}.
- Proxy data was deleted by {{Actor.Name}}.
- Proxy data was registered by {{Actor.Name}}.
- Proxy registration code was claimed by {{Actor.Name}}.
- Proxy registration code was created by {{Actor.Name}}.
- Proxy registration code was deleted by {{Actor.Name}}.
- Proxy registration code was modified by {{Actor.Name}}.
- Proxy state data was changed by {{Actor.Name}}.
- RADIUS server was deleted by {{Actor.Name}}.
- RADIUS configuration was created by {{Actor.Name}}.
- RADIUS server was created by {{Actor.Name}}.
- Cloud state in Directory Services was set by {{Actor.Name}}.
- User password was changed by {{Actor.Name}}.
- U2f device registration was completed by {{Actor.Name}}.
- U2f device was removed by {{Actor.Name}}.
- User's security question set was configured by {{Actor.Name}}.
- User's data was modified by {{Actor.Name}}.

Identity Federation Services

Identity Federation encompasses authentication that requires redirect to an external IDP.

Table of Contents

- Attribute mapping {{Target.Name}} added by {{Actor.Name}}
- Attribute mapping {{Target.Name}} deleted by {{Actor.Name}}
- Attribute mapping {{Target.Name}} updated by {{Actor.Name}}
- Authentication failed for {{Target.Id}}
- Authentication started for {{Target.Id}}
- Authentication succeeded for {{Target.Id}}
- Debugging started for {{Target.Name}} by {{Actor.Name}}
- Debugging logs viewed for {{Target.Name}} by {{Actor.Name}}
- Domain mapping {{Target.Name}} added by {{Actor.Name}}
- Domain mapping {{Target.Name}} deleted by {{Actor.Name}}
- Domain mapping {{Target.Name}} updated by {{Actor.Name}}
- Group mapping {{Target.Name}} added by {{Actor.Name}}
- Group mapping {{Target.Name}} deleted by {{Actor.Name}}
- Group mapping {{Target.Name}} updated by {{Actor.Name}}
- Oidc configuration {{Target.Name}} added by {{Actor.Name}}
- Oidc configuration {{Target.Name}} deleted by {{Actor.Name}}
- Oidc configuration {{Target.Name}} updated by {{Actor.Name}}
- Oidc configuration {{Target.Name}} viewed by {{Actor.Name}}
- Oidc configurations viewed by {{Actor.Name}}
- Saml configuration {{Target.Name}} added by {{Actor.Name}}
- Saml configuration {{Target.Name}} deleted by {{Actor.Name}}
- Saml configuration decryption Certificate {{Target.Name}} downloaded by {{Actor.Name}}
- Saml configuration Idp Certificate {{Target.Name}} downloaded by {{Actor.Name}}
- Saml configuration outbound metadata for {{Target.Name}} downloaded by {{Actor.Name}}
- Saml configuration signing Certificate {{Target.Name}} downloaded by {{Actor.Name}}
- Saml configuration {{Target.Name}} updated by {{Actor.Name}}
- Saml configuration {{Target.Name}} viewed by {{Actor.Name}}
- Saml configurations viewed by {{Actor.Name}}

MFA Providers Services

- Public preview opt-in settings were changed by {{Actor.Name}}.
- Public preview opt-in settings were changed by {{Actor.Name}}.

Permissions Services

This service category audits any updates to permissions configured on the platform. Service levels audited include the following.

- {{Actor.Name}} added a role membership.
- {{Actor.Name}} added a user to a role.
- {{Actor.Name}} removed a user from a role.

Policy Services

The following Policy services are audited:

- Policy had conditions added by user {{Actor.Name}}.
- Policy had conditions removed by user {{Actor.Name}}.
- Policy had conditions added by user {{Actor.Name}}.
- Policy was archived by user {{Actor.Name}}.
- Policy was created by user {{Actor.Name}}.
- Policy was deleted by user {{Actor.Name}}.
- Policy was disabled by user {{Actor.Name}}.
- Policy was enabled by user {{Actor.Name}}.
- Policy was redeployed by user {{Actor.Name}}.
- Policy configuration was updated by user {{Actor.Name}}.
- Policy had post tasks added by user {{Actor.Name}}.
- Policy had post tasks removed by user {{Actor.Name}}.
- Policy had post tasks updated by user {{Actor.Name}}.
- Policy had pre tasks added by user {{Actor.Name}}.
- Policy had pre tasks removed by user {{Actor.Name}}.
- Policy had pre tasks updated by user {{Actor.Name}}.
- Policy had remediation tasks added by user {{Actor.Name}}.
- Policy had remediation tasks removed by user {{Actor.Name}}.
- Policy had remediation tasks updated by user {{Actor.Name}}.
- Policy had rules added by user {{Actor.Name}}.
- Policy had rules removed by user {{Actor.Name}}.
- Policy had rules updated by user {{Actor.Name}}.
- Policy had subject groups added by user {{Actor.Name}}.
- Policy had subject groups removed by user {{Actor.Name}}.

Table of Contents

- Policy had subject users added by user {{Actor.Name}}.
- Policy had subject users removed by user {{Actor.Name}}.
- Policy had target groups added by user {{Actor.Name}}.
- Policy had target groups removed by user {{Actor.Name}}.
- Policy had target instances added by user {{Actor.Name}}.
- Policy had target instances removed by user {{Actor.Name}}.

Privileged Remote Access Services

The Privileged Remote Access (PRA) service levels audit all remote access events and include the following.

- Engine activated by user {{Actor.Name}}.
- Engine created by user {{Actor.Name}}.
- Installation script for engine created by user {{Actor.Name}}.
- Engines retrieved by user {{Actor.Name}}.
- Engine removed by user {{Actor.Name}}.
- Engine upgraded by user {{Actor.Name}}.
- Secrets retrieved by user {{Actor.Name}}.
- Session closed by user {{Actor.Name}} after disconnection.
- Session terminated from the vault and closed by user {{Actor.Name}}.
- Session for a secret launched by user {{Actor.Name}}.
- Clipboard data viewed by user {{Actor.Name}}.
- Clipboard data is sent to target by user {{Actor.Name}}.
- Clipboard data is copied by user {{Actor.Name}}.
- Site created by user {{Actor.Name}}.
- Sites retrieved by user {{Actor.Name}}.
- Site removed by user {{Actor.Name}}.
- Site updated by user {{Actor.Name}}.
- Templates retrieved by query by user {{Actor.Name}}.
- Template deselected by user {{Actor.Name}}.
- Templates selected by user {{Actor.Name}}.
- Vault information updated by user {{Actor.Name}}.
- Vault information viewed by user {{Actor.Name}}.
- File list retrieved by user {{Actor.Name}}.
- File uploaded by user {{Actor.Name}}.
- File downloaded by user {{Actor.Name}}.

Registration Services

- {{Actor.Name}} created a new registration code
- Registration Service has registered a new {{Target.Name}} workload
- {{Actor.Name}} generated a new device code
- Registration Service has completed a request to recover a workload's identity
- Service User has been provisioned for client {{Actor.Name}}
- Access Token has been generated for service user with client id {{Actor.Id}}

Secret Server Services

The Secret Server service monitors events related to Secret Server for any activity related to the Delinea Platform. The following levels are audited:

- Folder was added by {{Actor.Name}}.
- Folder was deleted by {{Actor.Name}}.
- Folder permissions were updated by {{Actor.Name}}.
- Secret {{Target.Name}} policy for folder was updated by {{Actor.Name}}.
- Secret {{Target.Name}} was deleted by {{Actor.Name}}.
- Secret {{Target.Name}} was viewed by {{Actor.Name}}.
- Secret {{Target.Name}} cache was viewed by {{Actor.Name}}.
- Secret {{Target.Name}} file was saved by {{Actor.Name}}.
- Secret {{Target.Name}} was updated by {{Actor.Name}}.
- Secret {{Target.Name}} was expired today for {{Actor.Name}}.
- Secret {{Target.Name}} will be expired in 1 day.
- Secret {{Target.Name}} will be expired in 7 days.
- Secret {{Target.Name}} will be expired in 15 days.
- Secret {{Target.Name}} will be expired in 3 days.
- Secret {{Target.Name}} policy was updated by {{Actor.Name}}.
- Secret {{Target.Name}} password was changed by {{Actor.Name}}.
- Secret {{Target.Name}} password change was failed.
- Secret {{Target.Name}} was exported by {{Actor.Name}}.
- Secret {{Target.Name}} will be expired in 30 days.
- Secret {{Target.Name}} will be expired in 45 days.
- Secret {{Target.Name}} will be expired in 60 days.
- Secret {{Target.Name}} will be expired in 90 days.

Table of Contents

- Session recording was viewed by {{Actor.Name}}.
- Secret was copied by {{Actor.Name}}.
- Secret was checked in by {{Actor.Name}}.
- Secret was checked out by {{Actor.Name}}.
- Secret access was approved by {{Actor.Name}}.
- Secret access was denied by {{Actor.Name}}.
- Unlimited admin was enabled by {{Actor.Name}}.
- Unlimited admin was disabled by {{Actor.Name}}.
- Secret export was run by {{Actor.Name}}.
- Secret import was run by {{Actor.Name}}.
- Expire all secrets command was run by {{Actor.Name}}.
- Secret template was created by {{Actor.Name}}.
- Secret template was edited by {{Actor.Name}}.
- Secret template was copied by {{Actor.Name}}.
- Field in a secret template was encrypted by {{Actor.Name}}.
- Field in a secret template was exposed by {{Actor.Name}}.
- Owners of a secret template were updated by {{Actor.Name}}.
- Access permissions for creating a secret template were updated by {{Actor.Name}}.
- Licenses will be expired in 30 days.
- Group owners were updated by {{Actor.Name}}.
- Secret policy was created by {{Actor.Name}}.
- Secret policy was updated by {{Actor.Name}}.
- Site was created by {{Actor.Name}}.
- Site was updated by {{Actor.Name}}.
- Site was enabled by {{Actor.Name}}.
- Site was disabled by {{Actor.Name}}.
- Site engine was added by {{Actor.Name}}.
- Site engine was removed by {{Actor.Name}}.
- Site engine was online for {{Actor.Name}}.
- Site engine was offline for {{Actor.Name}}.
- Site engine was downloaded by {{Actor.Name}}.
- Engine was created by {{Actor.Name}}.
- Engine was activated by {{Actor.Name}}.

Table of Contents

- Engine was deactivated by {{Actor.Name}}.
- Site connector was created by {{Actor.Name}}.
- Site connector was edited by {{Actor.Name}}.
- Site connector was enabled by {{Actor.Name}}.
- Site connector was disabled by {{Actor.Name}}.
- Credentials of a site connector were viewed by {{Actor.Name}}.
- Auto export settings were edited by {{Actor.Name}}.
- Auto export data was exported by {{Actor.Name}}.
- Auto export was run by {{Actor.Name}}.
- Auto export data was downloaded by {{Actor.Name}}.
- User was created by {{Actor.Name}}.
- User was disabled by {{Actor.Name}}.
- User was enabled by {{Actor.Name}}.
- User was locked out by {{Actor.Name}}.
- User was added to a group by {{Actor.Name}}.
- User was removed from a group by {{Actor.Name}}.
- User was removed from a group by {{Actor.Name}}.
- Logout was performed by {{Actor.Name}}.
- Login was failed for {{Actor.Name}}.
- Password was changed by {{Actor.Name}}.
- User owners were updated by {{Actor.Name}}.
- 2 Factor settings were updated by {{Actor.Name}}.
- A challenge was given to {{Actor.Name}}.
- Challenge for {{Actor.Name}} was cleared.
- Role was created by {{Actor.Name}}.
- A user or group was assigned to a role by {{Actor.Name}}.
- A user or group was unassigned from a role by {{Actor.Name}}.
- Role was enabled by {{Actor.Name}}.
- Role was disabled by {{Actor.Name}}.
- Role was updated by {{Actor.Name}}.
- Permissions were added to a role by {{Actor.Name}}.
- Permissions were removed from the role by {{Actor.Name}}.
- HSM encryption was enabled by {{Actor.Name}}.

Table of Contents

- HSM encryption was rotated by {{Actor.Name}}.
- HSM encryption was disabled by {{Actor.Name}}.
- Secret keys rotation for encryption was run by {{Actor.Name}}.
- Secret keys rotation for encryption was canceled by {{Actor.Name}}.
- Secret keys rotation for encryption was completed successfully by {{Actor.Name}}.
- Secret keys rotation for encryption failed for {{Actor.Name}}.
- Configuration was updated by {{Actor.Name}}.
- An IP address range was created by {{Actor.Name}}.
- An IP address range was updated by {{Actor.Name}}.
- An IP address range was deleted by {{Actor.Name}}.
- A user was added to the IP address range by {{Actor.Name}}.
- A user was removed from the IP address range by {{Actor.Name}}.
- A group was added to the IP address range by {{Actor.Name}}.
- A group was removed from the IP address range by {{Actor.Name}}.
- Secret heartbeat failed for {{Actor.Name}}.
- Secret heartbeat succeeded for {{Actor.Name}}.
- Secret hook run failed for {{Actor.Name}}.
- Secret hook run was completed by {{Actor.Name}}.
- A secret hook was created by {{Actor.Name}}.
- A secret hook was updated by {{Actor.Name}}.
- A secret hook was deleted by {{Actor.Name}}.
- A custom secret was audited by {{Actor.Name}}.
- Password of a secret was viewed by {{Actor.Name}}.
- Secret password was copied to the clipboard by {{Actor.Name}}.
- A secret dependency was removed by {{Actor.Name}}.
- A secret dependency was added by {{Actor.Name}}.
- A Powershell script was created by {{Actor.Name}}.
- A Powershell script was deactivated by {{Actor.Name}}.
- A Powershell script was updated by {{Actor.Name}}.
- A Powershell script was activated by {{Actor.Name}}.
- A Powershell script was viewed by {{Actor.Name}}.
- An SSH script was created by {{Actor.Name}}.
- An SSH script was deactivated by {{Actor.Name}}.

Table of Contents

- An SSH script was updated by {{Actor.Name}}.
- An SSH script was activated by {{Actor.Name}}.
- An SSH script was viewed by {{Actor.Name}}.
- An SQL script was created by {{Actor.Name}}.
- An SQL script was deactivated by {{Actor.Name}}.
- An SQL script was updated by {{Actor.Name}}.
- An SQL script was activated by {{Actor.Name}}.
- An SQL script was viewed by {{Actor.Name}}.
- A domain was added to the site by {{Actor.Name}}.
- A domain was removed from the site by {{Actor.Name}}.
- Engine was disconnected.
- Engine was connected.
- A dual control was created by {{Actor.Name}}.
- A dual control was updated by {{Actor.Name}}.
- A dual control was deleted by {{Actor.Name}}.
- A secret was activated by {{Actor.Name}}.
- A secret was created by {{Actor.Name}}.
- A secret was deactivated by {{Actor.Name}}.
- An erase of a secret was requested by {{Actor.Name}}.
- A secret was launched by {{Actor.Name}}.
- A web session for a secret was launched by {{Actor.Name}}.
- A failed secret dependency was encountered by {{Actor.Name}}.
- Secret view was edited by {{Actor.Name}}.
- A secret password requirement was added by {{Actor.Name}}.
- Secret password requirement was removed by {{Actor.Name}}.
- Secret password change was unsuccessful.
- Engine was deleted by {{Actor.Name}}.
- Security analytics configuration was updated by {{Actor.Name}}.
- Secret settings were exported by {{Actor.Name}}.
- Secret settings were imported by {{Actor.Name}}.
- User was updated by {{Actor.Name}}.
- 2 Factor settings were reset by {{Actor.Name}}.
- Failed to reset the 2 Factor settings by {{Actor.Name}}.

Table of Contents

- Personally identifiable information was removed by {{Actor.Name}}.
- A license was added by {{Actor.Name}}.
- A license was deleted by {{Actor.Name}}.
- Password changer was created by {{Actor.Name}}.
- Password changer was updated by {{Actor.Name}}.
- Password changer was enabled by {{Actor.Name}}.
- Password changer was disabled by {{Actor.Name}}.
- A command on the password changer was updated by {{Actor.Name}}.
- A command on the password changer was created by {{Actor.Name}}.
- A command from the password changer was deleted by {{Actor.Name}}.
- Authentication on the password changer was updated by {{Actor.Name}}.
- The scanned field on the password changer was updated by {{Actor.Name}}.
- Password requirement was created by {{Actor.Name}}.
- Password requirement was edited by {{Actor.Name}}.
- Domain was created by {{Actor.Name}}.
- Domain was updated by {{Actor.Name}}.
- Group was created by {{Actor.Name}}.
- Group was edited by {{Actor.Name}}.
- Key management encryption was enabled by {{Actor.Name}}.
- Key management encryption was updated by {{Actor.Name}}.
- Key management encryption was disabled by {{Actor.Name}}.
- Data replication for disaster recovery was successful by {{Actor.Name}}.
- Data replication for disaster recovery was initiated by {{Actor.Name}}.
- Data replication for disaster recovery failed for {{Actor.Name}}.
- Data replica for disaster recovery was created by {{Actor.Name}}.
- Data replica for disaster recovery was approved by {{Actor.Name}}.
- Data replica for disaster recovery was disabled by {{Actor.Name}}.
- Data replica for disaster recovery was deleted by {{Actor.Name}}.
- Data replica for disaster recovery was unapproved by {{Actor.Name}}.
- Data replica folder for disaster recovery was updated by {{Actor.Name}}.
- Configuration was upgraded by {{Actor.Name}}.
- Configuration was backed up by {{Actor.Name}}.
- Configuration database was updated by {{Actor.Name}}.

Table of Contents

- TLS failed for {{Actor.Name}}.
- Domain was synchronized by {{Actor.Name}}.
- Secret pre-checkout was run by {{Actor.Name}}.
- Secret pre-checkin was run by {{Actor.Name}}.
- SSH proxy for the site was enabled by {{Actor.Name}}.
- SSH proxy for the site was disabled by {{Actor.Name}}.
- RDP proxy for the site was enabled by {{Actor.Name}}.
- RDP proxy for the site was disabled by {{Actor.Name}}.
- Site proxy endpoint was updated by {{Actor.Name}}.
- Engine proxy endpoint was updated by {{Actor.Name}}.
- Security application hardening for secret settings was enabled by {{Actor.Name}}.
- Security application hardening for secret settings was disabled by {{Actor.Name}}.
- Security application hardening for secret settings was bypassed by {{Actor.Name}}.
- Security application hardening for secret settings was updated by {{Actor.Name}}.
- MEK rotation for encryption was initiated by {{Actor.Name}}.
- MEK rotation for encryption was retried by {{Actor.Name}}.
- The MEK for encryption was successfully rotated by {{Actor.Name}}.
- MEK rotation for encryption failed for {{Actor.Name}}.
- SSH proxy was enabled by {{Actor.Name}}.
- SSH proxy was disabled by {{Actor.Name}}.
- RDP proxy was enabled by {{Actor.Name}}.
- RDP proxy was disabled by {{Actor.Name}}.
- Node proxy endpoint was updated by {{Actor.Name}}.
- Disaster recovery configuration was updated by {{Actor.Name}}.
- Character set was created by {{Actor.Name}}.
- Character set was updated by {{Actor.Name}}.
- Character set was enabled by {{Actor.Name}}.
- Character set was disabled by {{Actor.Name}}.
- Backup configuration was updated by {{Actor.Name}}.
- Backup failed for {{Actor.Name}}.
- Platform synchronized.

Session Recording Services

The Session Recording service levels indicate any actions involving the audit of a recording.

- Session recording has detected an anomaly
- Session recording has been deleted
- Session recording has been downloaded
- Session recording is flagged
- Session recording {{Target.Id}} viewed by user {{Actor.Name}}.

Tenant Profile Services

- Public preview opt-in settings were changed by {{Actor.Name}}.
- Public preview opt-in settings were changed by {{Actor.Name}}.

Analytics



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

Analytics on the platform empowers IT and security administrators to prevent, detect, and stop breaches by continually monitoring alerts across the organization to identify early signs of threats.

Permissions

These permissions are required to view and manage alerts on the Alerts page, as well as the Analytics Dashboard. Permissions are assigned to a role, then the role is assigned to a user. Refer to "Roles and Permissions" on page 203.

View Alerts - allows you to view all alerts on the Alerts page. From the dashboard, click the linked title in the Latest Alerts pane.

Update Alerts - allows you to mark false positives for alerts.

Manage Alerts - allows you to view the Risk Analysis page and the Risk Configuration page, where risk scores are managed and defined.

Identifying Alerts

Alerts identify any deviations from expected configuration or a baseline of your Delinea Platform tenant. The mechanism that identifies alerts runs continuously in your environment. Alerts help administrators and other staff members learn to recognize trends and better respond to security threats.

Based on the data available in activities like IP address and user agent, the platform can determine anomalous locations or user agents. By tracking those activities over time and correlating them with user historical data and actions, the platform can determine a baseline of user activity for their common locations, IP addresses, browsers used, and so on.

The data can also be used to identify authentication attack attempts like brute force and MFA bombing. While analytics generate alerts to highlight those findings each time something is detected, the end result is user risk. The risk assessment reflects the sensitivity of the account based on those findings.

Analytics Dashboard



Note: This feature is currently available only to customers participating in a Public Preview. For details, see ["Public Preview"](#) on page 76

Click **Home** from the left navigation, then **Dashboards**. **Analytics Dashboard** presents multiple panes of information that provide at-a-glance data visuals of alerts over days, weeks, or months.

Interpreting Dashboard Analytics

Current Risk Score

The **Current Risk Score** displayed at the top of the page represents the risk across the platform based on the average risk of all users who have been assigned a risk score. Users that have no risk score assigned are not considered in the calculation.

Riskiest Accounts

This list reflects the top five users at highest risk in the Platform, along with their risk level. Click any user to view their account details. Refer to ["Users and Groups"](#) on page 169.

Latest Alerts

This list shows the five latest alerts, their type, and severity. Severity is a system-defined value assigned to each individual alert type.

Click Latest Alerts in the title of the pane to access the Alerts page in the [Threat Center](#).

Alerts Over Time

This graph provides administrators with a visual representation of the number of alerts created each day over the last 30 days. Individual plots are created for each alert level. Hover over any data point to view its alert total.

Activity

The following panes provide identification of deviations or spikes in activity. This activity reflects interaction with the system.

- **Most Active Users** - the most active users in the platform, based on their activities in the last 60 days.
- **Most Active Secrets** - the most active secrets are based on view activity for the secrets. The secret name only displays if the user has permissions to view the secret; otherwise, the ID is displayed.
- **Top User Agents** - the most active agents, based on users sessions (activity time frame in the Platform).
- **Top Active IPs** - the most active IPs, based on users sessions (activity time frame in the Platform). Click on any secret or IP listed to view its details page.

Analytics Findings and Risk



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

Analytics generate alerts based on different rules, the deviation from those rules, or any risk detected on the account. For example, an alert could be generated when an attempt is made to guess the account password.

Based on the alerts that are triggered for each user, the Delinea Platform calculates the risk of the platform account. This risk is taken into account only if the alert is unresolved. The analytics feature calculates a risk score for each user: low, medium, high, or N/A if no alerts were found for the user.

Refer to the "Threat Center" on page 724 for basic information regarding alerts.

Risk Scores

Risk is shown in the **Risk Score** column in the Users table. (From the left navigation, select **Access > Users**.) For more information about the Users table, see [Managing User Accounts](#).

You can select a user from the list to view a details page, then select the **User risk** tab. This tab shows the user's risk score and the alerts that contributed to the score. If the risk exists and has alerts, you can review how each alert contributes to the user risk from this page to understand why it was triggered.

Types of Alerts

The following table explains the types of alerts.

Alert Name	Description	Logic
Login on weekend	User login during a weekend	Trigger an alert if a user logs in on Sunday or Saturday. Filter out users who are active on two or more consecutive weekends.
User performed an activity from an abnormal location	User performed an activity from a location where they are not normally found	Based on the session IP, compare the session location to the user's previous locations (at least 10 days of baseline required) and alert if the location is new. Ignores IPs with unknown locations.
Irregular session	The user sessions started before or after the user's usual activity time, determined by the user timeline	Baseline data is collected for at least 14 days of activities. Based on this baseline, determine the user's usual start time and end time, as one standard deviation from start and end time. Each session occurring outside of those thresholds triggers an alert.

Table of Contents

Abnormal spike in users activity	The user performed more than five times their normal activities	<p>Determine whether the baseline of at least 14 days of platform usage exists for the user. If the baseline exists, calculate a baseline of activities, excluding some like login/MFA and secret view.</p> <p>Trigger an alert if the user's non-excluded platform actions exceed five times the number of average activities.</p>
Brute force	Attempt was made to brute force an account	<p>Detect any of these events:</p> <ul style="list-style-type: none"> ■ Login burst: Excessive login attempts from the same account within an hour. You can configure the minimum number of attempts. ■ Low and slow: Authentication attempts are spread over days, weeks, and months. Detects multiple failed attempts to log in; for example, 10 failed attempts over a week. ■ Distributed: Login attempts are sent from multiple IP addresses to remain below the detection threshold. This can involve thousands of IPs, with as few as one or two attempts per IP. <p>This method is detected by analyzing all attempts on each account, grouping them by IP and user agent, and finding a pattern of failed attempts from multiple sources over a short period of time. This indicates a distributed attack where multiple sources are failing at the same time or during a short time, such as a single day.</p>
Account under MFA bombing attack	Detects MFA bombing events and repeated attempts to access an account that requires MFA authentication	<p>Detect MFA bombing by performing the following:</p> <ol style="list-style-type: none"> 1. Fetch recent MFA login activities, both accepted and rejected. 2. Group events by the initiator IP address. 3. For each unknown IP, create an incident if: <ul style="list-style-type: none"> ■ Authentication was denied more than it was approved, or ■ Denial attempts exceed a system-defined threshold.
Inactive user performed an action	Triggered if a dormant account for at least 90 days performed an activity	Per each non enabled account, we search for actions that occurred after a period of 90 days or more of inactivity, meaning in this time period, the system did not record any activity for the user.

Discovery

Discovery is a powerful feature designed to help organizations discover and manage privileged accounts, credentials, and other sensitive information across their IT infrastructure. It enables IT teams to gain visibility into all of their systems, applications, and devices, and identify potential security risks and vulnerabilities.

Although the [Discovery](#) feature runs from Secret Server, all customers of Delinea Platform with integrated Secret Server, including [Delinea PCS](#) and [ITP/PCCE](#) customers, can use Discovery directly from the platform.

By scanning and analyzing systems and applications, discovery can detect and classify privileged accounts and credentials, including those that are inactive. You can automatically find local Windows accounts, Active Directory services, Unix, VMware ESX/ESXi, and Active Directory domain accounts.

See also "Continuous Identity Discovery" on page 738, a subset of the Delinea Platform's [ITP/PCCE](#) features.

Combined Discovery



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

The Combined Discovery feature enables users to see **Vault** sources from Secret Server alongside **Identity Protection** sources from the Delinea Platform.

1. From the left navigation menu, click **Discovery**, then select **Sources**.

On the Sources page, all Delinea Platform users with integrated Secret Server will see two types of discovery sources in the table: Vault sources and Identity Protection (ITP) sources. The ability to see Vault sources from Secret Server alongside Identity Protection sources from the Delinea Platform is known as **combined discovery**.

A

Home

Secret Server

Inventory

Insights

Discovery

Policies

Identity Posture

Threat Center

Access

Marketplace

Inbox

Settings

<<

Discovery

Sources

Vault

Analysis

Network view

Configuration

Logs

Computer scan logs

Q Search

?

☆

🔔

●

Sources ☆ 🔗

Create source

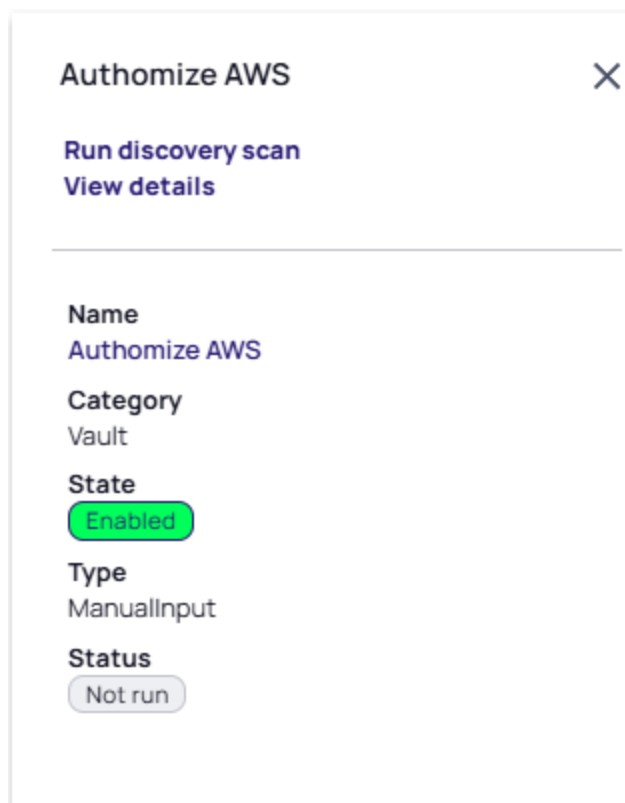
🔍 Name ⬇️ 🔗

14 items

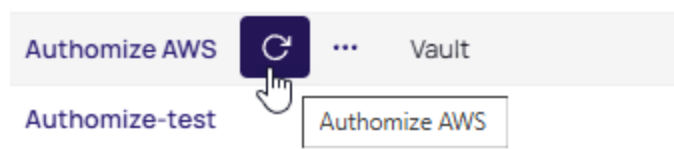
NAME ↑	CATEGORY	STATE	STATUS ↑	TYPE	LAST RUN
AWS 67	Identity Protection	Enabled	Authorization Error	AWS	
AWS	Identity Protection	Enabled	Authorization Error	AWS	
MSFT	Identity Protection	Enabled	Synced	Entra ID and Azure	11 hours, 44 Minutes ago
Okta	Identity Protection	Enabled	Synced	Okta	7 hours, 58 Minutes ago
Authomize AWS	Vault	Enabled	Not run	ManualInput	
Authomize-test	Vault	Enabled	Not run	ManualInput	
PM-XPM-Domain	Vault	Enabled	Synced	ActiveDirectory	3 hours, 2 Minutes ago
test 2	Vault	Enabled	Synced	ManualInput	3 hours, 2 Minutes ago

If you are an ITP/PCCE customer, you can create new Identity Protection sources. If you are not an ITP/PCCE customer, you cannot create new Identity Protection sources, but you can click to be taken to the Delinea Marketplace to learn more about them.

2. To see basic information about a discovery scan, click anywhere in the scan row to open a panel to the right.



3. To see detailed information about the scan, click **View Details** in the right panel or click the name of the scan in the row.
4. To run the vault discovery scan, click **Run discovery scan** in the right panel or hover your cursor over the scan row to the right of the source name, and click the forward circle icon.



A dialog will appear with options for the scan.

Run vault discovery

When triggered, vault discovery will run against all vault discovery sources.

Run discovery

Scan networks to discovery hosts to scan.



Last ran: 3 hours, 34 Minutes ago

Run computer scan

Scan all discovered hosts for accounts.



Last ran: 2 hours, 48 Minutes ago


Cancel


Run now


- 5. When you are satisfied with the options you have chosen, click **Run now**. It might take a minute or two for the Discovery Scan to complete.
- 6. You can also click **Create source** to create a new vault discovery source.


Create discovery source


Vault ▾



Active Directory



Unix


VMWare ESX/ESXi


AWS (Amazon Web Services)


GCP (Google Cloud Platform)


Entra ID



A vault discovery source will find computers, accounts, services, keys, and other items that can be taken over and managed securely through password rotation and dependency control.

Cancel

Continue

For more information about discovery in Secret Server, see the following topics in the Secret Server documentation:

- [Discovery Overview](#)
- [Introduction to Discovery Sources, Scanners, and Templates](#)
- [Running and Interpreting Active Directory Discovery](#)

Delinea Delinea Platform

Administrator Guide

Page 168 of 846

Users and Groups

To manage users on the Delinea Platform, begin by clicking **Access** from the left navigation menu, then selecting **Users**. The Users page displays all users on the platform, including Active Directory, Federated, and Delinea Directory (local) users.

Q Search

?

k

Users ☆ ↗

Add and manage user accounts. [Learn more about User Management](#)

More ▾Add Local User

▽ Q Search...

Statuses All statuses ▾ ×

Sources All sources ▾ ×

Users Users ▾ ×

Add filter

176 items

Username

Display Name

Email Address

Directory Source

Status

Last Invite

Last Login


Members

Risk Score

<input type="checkbox"/>	██████████	██████████	Delinea Directory	Active	08/10/2023 0...	08/18/2023 02...	Employee	Low
<input type="checkbox"/>	██████████	██████████	Active Directory (P...	Created			Employee	Low
<input type="checkbox"/>	██████████	██████████	Delinea Directory	Active	11/05/2024 12:...	01/10/2025 02...	Employee	Medium
<input type="checkbox"/>	██████████	██████████	Delinea Directory	Active	09/18/2024 12...	10/09/2024 0...	Employee	Low
<input type="checkbox"/>	██████████	██████████	Delinea Directory	Active	07/03/2024 0...	08/28/2024 0...	Employee	Low
<input type="checkbox"/>	██████████	██████████	Delinea Directory	Active	07/01/2024 11:...	01/10/2025 08...	Employee	High

Click a **USERNAME** to go to that specific user's page, where you can view and edit settings for the user account, including the user's group memberships, roles, policies, activities, and attributes. For detailed instructions on managing platform users, see [Managing User Accounts](#).

Risk Score

 **Note:** This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

Risk Score is displayed for each user. Risk is based on the analytics that generate non-resolved alerts and the associated findings. Risk scores are assigned as **Low**, **Medium**, and **High**. Refer to "Analytics Findings and Risk" on page 163.

Risk Level	Definition
N/A	No risk has been identified for this user. Our monitoring systems have not detected any suspicious behavior or security concerns.

Low	Minor security alerts have been triggered for this user. These alerts are typically low concern and may result from legitimate activities, such as accessing resources from an unusual geographic location. No immediate action is required, but continued monitoring is recommended.
Medium	Elevated risk indicators have been observed for this user. This may include multiple alerts or behavioral patterns that warrant further investigation. While the situation is not critical, proactive measures, such as enhanced monitoring or verifying the user's activity, are advised.
High	<p>Significant risk indicators have been detected for this user. Examples include:</p> <ul style="list-style-type: none">▪ Multiple suspicious actions on the account▪ An MFA (multi-factor authentication) bombing attempt followed by further anomalous activity <p>For high-risk situations, the following actions are strongly recommended:</p> <ul style="list-style-type: none">▪ Enforce a more secure MFA method for the user (e.g., hardware tokens or app-based authentication).▪ Collaborate with the user to identify and mitigate potential risks.▪ Take immediate steps to prevent account takeover attempts.

External User Accounts vs. Local User Accounts

Virtually every user account on the platform should be an external user account, meaning either an Active Directory account or a federated account.

A local user account is added directly to the platform by an administrator.

An external user account isn't added directly to the platform, but becomes accessible on the platform when the associated Active Directory or federation is connected to the platform.

The administrator must still provide permissions to the user to access platform features.

A local user must satisfy local authentication requirements to log in to the platform.

An external user must only satisfy the authentication requirements through the external source (AD or federation IdP).

A local user account appears on the Users page (**Access > Users**) when an administrator adds the account to the platform.

An external user account appears on the Users page only after the user logs in to the platform for the first time.

Avoid Adding Local User Accounts

Adding local user accounts to the platform is not considered a best practice for privileged access management. Local user accounts should be added only rarely, and for very specific purposes. For example, you might need to add a local user account for someone who needs to try out platform functionality for a very limited time. Vendors are also added as local accounts. For details, see [Adding Local User Accounts](#).

For related content, see the following:

- [Managing User Accounts](#)
- [Managing Your User Profile](#)
- [Managing Vendor Entitlements with Active Directory](#)


Adding Users


You can add local users directly to the platform. You can also add non-local users from Active Directories and Federation providers.

Adding Local Users

Adding local users to the platform is not considered a best practice for privileged access management. Local user accounts should be added only rarely, and for very specific purposes. For example, you might need to add a local user account for someone who needs to try out platform functionality for a very limited time. Vendors are also added as local users.

Typically, the Delinea Platform is used by a corporate enterprise to manage privileged access for their employees and contractors. A local user would typically be added by a platform administrator, but a platform administrator is not legally authorized to formally establish a person's identity. Only human resources personnel are legally authorized to formally establish a new employee's identity, for example by confirming their proof of residency, asking to see their driver's license or work visa, and taking their photograph. And only human resources can authorize that person to be added as a new employee to the corporate Active Directory, and to authorize their removal from the employee Active Directory.

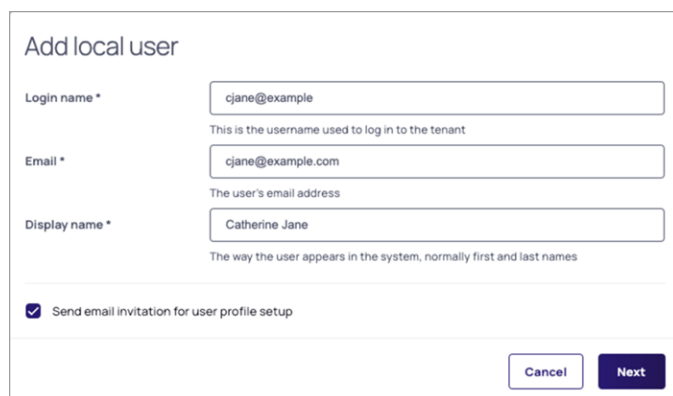
 **Note:** Local users cannot be converted to external (Active Directory or federated) users.

 **Note:** (Migration customers only) After the Connector is installed and Active Directory is set up on the platform, do not add an existing Secret Server user as a local platform user, because doing so could cause synchronization issues between the platform and Secret Server.

Add Local Users

1. Click **Access** from the left navigation, then select **Users**.
2. The Users page displays each user on a row, with columns showing basic user information including the user's Display Name, Email, Source, Status, Last Invite, and Last Login.
3. Click **Add Local User** on the right to create a new local user.
4. On the Add local user page, fill in the required fields for **Login name**, **Email**, and **Display name**,

Users and Groups

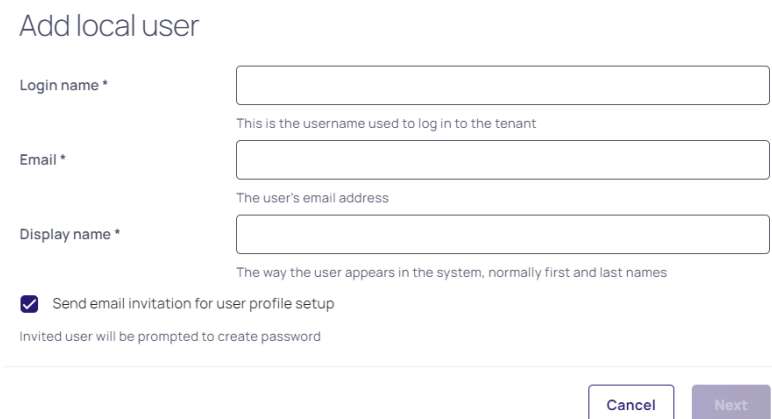


The screenshot shows the 'Add local user' form with the following fields and values:

- Login name ***: cjane@example
This is the username used to log in to the tenant
- Email ***: cjane@example.com
The user's email address
- Display name ***: Catherine Jane
The way the user appears in the system, normally first and last names
- ☒ **Send email invitation for user profile setup**

At the bottom right are two buttons: 'Cancel' and 'Next'.

The checkbox **Send email invitation for user profile setup** is selected by default. If you leave this option selected, the user will automatically receive an email containing an **Accept** button, with a one-time password embedded in the button. When the user clicks the button, they are taken to the platform and automatically logged in with the one-time password. They are then required to immediately change the password to log in again.



The screenshot shows the 'Add local user' form with empty fields:

- Login name ***: [Empty field]
This is the username used to log in to the tenant
- Email ***: [Empty field]
The user's email address
- Display name ***: [Empty field]
The way the user appears in the system, normally first and last names
- ☒ **Send email invitation for user profile setup**
Invited user will be prompted to create password

At the bottom right are two buttons: 'Cancel' and 'Next'.

If you choose to deselect **Send email invitation for user profile setup**, a panel opens where you can set a password for the user either manually or automatically. The user will not receive an email invitation to log in to the platform in this case, and you will need to copy and save the password and deliver it to the user some other way.

5. Click **Next**.
6. The Advanced Settings window appears. The default **Membership Type** is set to *Employee*. This can later be changed to *Vendor*. See "Advanced Settings " on page 184 for more information. After you have selected the correct membership type, click **Next**.

Users and Groups

Advanced Settings

These advanced settings are optional. You can skip this step and adjust these settings after the user has been created.

Membership type

Employee (default)

Employee (default)

Vendor

Cancel

Previous

Next

7. Add the new user to a group, if needed.

Add user to groups

Q Search...

8 items

GROUP NAME ↑

DESCRIPTION

<input checked="" type="checkbox"/>	Everybody	All authenticated users
<input type="checkbox"/>	Group using RCOAUTH profile	Testing
<input type="checkbox"/>	Hachey Test Group	
<input type="checkbox"/>	Hachey Test Group2	rewgtew
<input type="checkbox"/>	pk-group	
<input type="checkbox"/>	Platform Group to Sync to SSC	Group to test Platform Group Sync to SSC


Cancel

Previous

Add

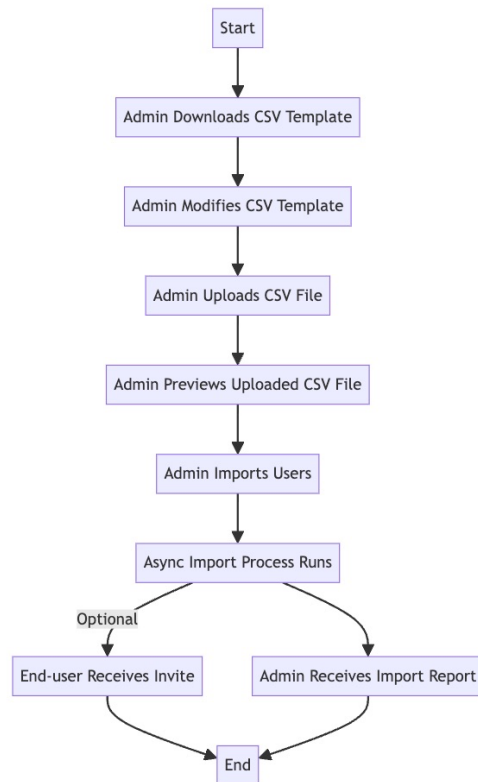
Bulk Importing Local Users

With the bulk import feature, administrators can import a large number of local users in a single operation, rather than manually adding each user one by one to the Delinea Directory. This feature saves administrators time and effort by eliminating repetitive data entry and reducing errors. Additionally, it supports a CSV format template, allowing for offline preparation of user data, which can be efficiently organized before import.

 **Note:** The platform does not natively support bulk import and synchronization of all users from an external source such as AD, or from a federation service. Platform administrators can find AD users to add to the platform by performing filtered searches through external AD directories, but federated directories cannot be searched.

Workflow:

Users and Groups



Steps:

1. Log in to the platform.
2. Click **Access** from the left navigation, then select **Users**.
3. In the Users section, click **Import Users**.
4. Download the provided CSV template by clicking the respective option.
5. Open the downloaded CSV template and update it with the user account information you wish to add. Refer to the following guidelines:
 - All required fields must be present.
 - Each field must have a header.
 - Headers must match exactly as shown in the following table, including uppercase characters and spaces.
 - Attributes not listed in the following table must be defined in **Settings > User attributes > Additional attributes**. If the additional attributes are not defined, they will not be uploaded. The attribute names you define on the Additional Attributes page must exactly match the corresponding headers in the CSV file.

Default Fields	Rules
Login Name	Required - Enter the full username, including the login suffix, in the form <login name>@<loginsuffix>. The login suffix must already exist.
Email Address	Required - You can specify one email address only. The email address must be of a valid form. Plain text strings, such as "N/A" or "unavailable", are not allowed.
Display Name	Optional - You can enter the display name in Excel using either format: first last or last, first. If you are editing the CSV file, use quotes if you specify the last name first (for example, "last, first"). This field is optional, but highly recommended.
Description	Optional - A description of the user. Do not use punctuation. The limit is 128 characters.
Office number Mobile number Home number	Optional - You must enter the area code. You can enter domestic U.S. numbers in the following forms: <ul style="list-style-type: none"> • 1234567890 • 123-456-7890 To enter an international number, use E.164 number formatting . If you use the phone or text message options for multi-factor authentication, the Office and/or Mobile numbers must be accurate. If the numbers are not accurate, the user cannot log in.
Groups	Optional - All regular users are automatically added to the Everybody group. You can specify multiple groups. Use commas to separate the groups. If you are editing the CSV file, surround the groups with quotes; for example, "group1,group2,group3". The group must already exist, and the names are case-sensitive. Service users are excluded from the Everybody group.
Expiration Date	Optional - Enter a date when the user account expires. If you do not set a date, the account does not expire. This field is not in the CSV template.
Password	Optional - Sets the password for the user. Password requirements are based on the password policy settings in Access > Identity Policies > [User] > User security > Password settings .

Default Fields	Rules
Require Password Change	Optional - Specifies whether users must change the password upon the first successful login. The supported inputs are: False, f, no, n -- No password change required True, t, yes, y -- Password change required
Platform User Membership Type	Optional - By default, the membership type is <i>Employee</i> . If you are adding vendors, be sure to change the membership type to <i>Vendor</i> .
Reports to	Optional - Name of the reporting manager. This field is not in the CSV template.

- After updating the CSV template, return to the platform to upload the CSV file. Follow the same steps as before if you have exited from the Import Users flow. The file to upload must be: in CSV format, with a max size of 100 KB.
- Proceed by clicking **Next**.
- Review the first 15 records displayed in the preview. Use this opportunity to ensure that the entries are correctly formatted.
- Once reviewed, click **Next** to proceed.
- By default, the option Send email invite for user profile setup will be selected. If you wish to proceed with this option, the user will automatically receive an email invite to log into the platform. They will be prompted to change their password immediately upon login.
- Finally, click the **Import** button to initiate the import of the users.

The user import process operates asynchronously and the duration of completion depends on the number of users being added. Following the import, two email messages will be dispatched:

- **Bulk import report:** Sent to the initiating Admin, this email provides details on the number of new users specified in the file and the successful additions. Additionally, explanations are given for any failed user import.
- **Platform Invite:** Sent to each newly created user if the "Send email invite for user profile setup" option was chosen. This email contains a link that directs users to the platform, where they can set up a new password unless configured otherwise.

Service Users

Service users are specifically designed for non-interactive, programmatic access to the platform. They are intended for scenarios such as API integrations and automation scripts. Service users are not associated with regular users, and they are intentionally excluded from the predefined **Everybody** user group.

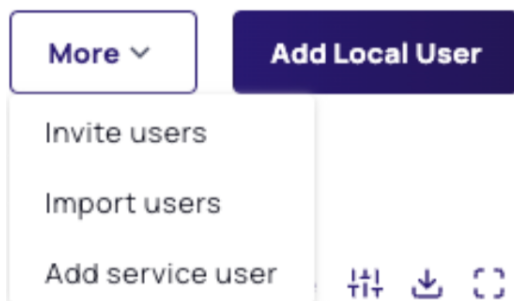
Key Points:

Users and Groups

- Service users are not added to the predefined **Everybody** group. For more information on predefined groups, see [Group Management](#).
- Service users have no permissions by default. Add the user to the appropriate group or role to give it only the permissions it needs for its headless use case.
- Service users cannot be invited like regular users; an administrator must manually create and configure them.
- When a service user is created, a corresponding application account is automatically generated in Secret Server, requiring no additional actions.
- Service users can log in interactively through the platform UI by default. You can disable this feature through Identity policies by selecting the **Disable interactive service user login** option. For details, see "Creating Identity Policies" on page 480.
- MFA is not applicable for non-interactive service users.

Add Service Users

1. Click **Access** from the left navigation menu.
2. Select **Users** to view the list of existing users.
3. On the Users page, click **More** in the top-right corner.
4. From the drop-down menu, select **Add service user**.



5. Complete the required fields on the **Add service user** form:
 - **Username**: A unique identifier for the service user.
 - **Email address**: This field is optional.
 - **Display name**: A descriptive name for the service user, typically reflecting its purpose.

- **Set password:** Set a secure password for the service user (Manual or Generated).

Add service user

Username *
This is the username used to log in to the tenant


Email address
The user's email address

Display name *
The way the user appears in the system, normally first and last names

Set password

☐ Manual ☒ Generated

A strong password is auto-generated that provides greater security.

Password * 

6. Assign the service user to the appropriate group based on its intended role and permissions.

Add user to groups

Use groups to categorize users and for assigning permissions.

25 items Group Name

<input type="checkbox"/>	GROUP NAME ↑	DESCRIPTION
<input type="checkbox"/>	A-Group1	
<input type="checkbox"/>	A-Group2	Group for Service User accounts to access pro...
<input type="checkbox"/>	A-Group3	
<input type="checkbox"/>	A-Group4	
<input type="checkbox"/>	A-Group5	
<input type="checkbox"/>	Everybody	All authenticated users
<input type="checkbox"/>	Svc-Group7	

7. Save the service user details.
8. Verify that the service user appears on the Users list.
9. Click the service user name in the Users list to open the user page and ensure that the user has the correct groups and permissions assigned.

Users and Groups

service-user@example

Overview

Groups

Roles

Additional attributes

Activity

Policy summary

Secret Server Settings

Some properties may be set to read-only by the directory service source. [Learn more about user profiles.](#)

Status

Created

Status description

User has been Created, but not yet logged in

Directory source

Delinea Directory

Created on

12/11/2024 12:39 pm

Last login

Last password change

12/11/2024 12:39 pm

Account

Service user

Yes

Display name

My Service User

Username

service-user@example

Email address

—

Description

—

Advanced Settings

Password never expires

No

Account is disabled

No

Account is locked

No

Account expires

Never

Secret Server details

User type

None

Enabled

No

Slack

None

Managing User Accounts

This page explains how to perform various administrative tasks to manage the user accounts in the Delinea Platform.

View User Accounts

To view a list of user accounts, click **Access** from the left navigation menu, then select **Users**. From the Users page, you can see all users on the platform in one place, including Active Directory, Federated, and local (Delinea Directory) users.

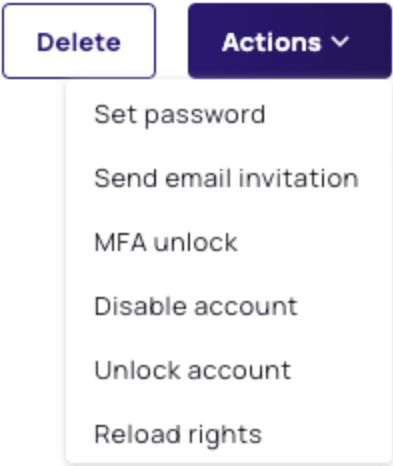
Click a specific **User Name** to open that user's account page, where you can view all information about that user and edit some of the user settings, including the user's group memberships, roles, policies, and attributes.

The top right of every tab on the user page has a **Delete** button and an **Actions** drop-down button.



To delete the user, click **Delete**.

To take common actions, click the **Actions** drop-down button.



The following table describes the available actions.

Action	Description
Set password	Prompts you to reset the user's account password. In the window that appears, enter a new password for the user.
Send email invitation	Sends an email to the selected user. As part of this workflow, the user is required to change their password the next time they log in.
MFA unlock	Suspends multi-factor authentication for 10 minutes. Multi-factor authentication requires users to perform additional steps, such as verifying their identity by email or phone call, to log in to the Delinea Platform. If the user is having trouble logging in, select the user and select this action to let the user log in with just a login name and password.
Disable account	Disable a user account. The disabled user is unable to log in to the platform. If the user is currently logged in, the user will not be able to access platform services that require authentication.

Users and Groups

Action	Description
Unlock account	When a user account is locked temporarily or permanently, which is usually triggered by specific policies or conditions, this action enables an administrator to unlock the account immediately. This action is only available when a local user account is locked.
Reload Rights	Enables the immediate reloading of a user's cached identity from their directory service, eliminating the need to wait for synchronization. This action is especially useful when user details have been updated in the remote directory service but have not yet been reflected in the platform.

Overview Tab

The individual user page opens by default to the **Overview** tab.

The screenshot displays the Delinea Platform user management interface. On the left is a sidebar with navigation icons for Access, Users, Groups, Roles, Identity policies, Secret Server, Inventory, Insights, Discovery, Policies, Identity Posture, Threat Center, Access, Marketplace, Inbox, and a back arrow. The main content area is titled 'Administration > User Management > Users' and includes a search bar 'Search the Delinea Platform'. Below the breadcrumb is the user email 'artdecco@mycompany' and a tabbed interface with 'Overview' selected. The 'Overview' tab shows 'Last password change' and an 'Account' section with fields for Display name (Art Decco), Username (* artdecco@mycompany), Email address (* artdecco@mycompany.com), Mobile phone, Office phone, Home phone, and Description. Below these are 'Manager' (Assign manager) and 'Profile photo' (Upload). At the bottom are 'Cancel' and 'Save' buttons. The 'Advanced Settings' section includes Membership type (Employee), Password never expires (No), Require password change at next login (Yes), Is a service user (No), Account is disabled (No), and Account is locked (No). The 'Secret Server details' section includes User type (None), Enabled (No), and Slack (None).

The top of the Overview tab displays the user account's basic information, including status, directory source, creation date, last login, and last password change.

Users and Groups

Overview

Groups

Roles

MFA redirection

Additional attributes

Activity

Policy summary

Secret Server Settings

Delete

Actions

Some properties may be set to read-only by the directory service source. [Learn more about user profiles.](#)

Status

Status description

Directory source

Created on

Last login

Last password change

Active

User is currently Active

Delinea Directory

08/10/2023 08:23 pm

08/09/2024 12:53 pm

03/03/2024 12:57 pm

Status

The following table provides descriptions of each status that can apply to a user.

Status	Description
Active	The user has logged in to the Delinea Platform.
Invited	An administrator has sent an invitation to a user, but the user has not accepted and logged in yet. You can send an invitation when you create a local account or after the user is created. When the user accepts the invite, the user will be prompted to reset their password before they are able to log in to the platform.
Created	The account was created on the platform, but no email invitations have been sent. Successfully provisioned users appear on the Users page with a status of Created.

Status	Description
Suspended	<p>The user account is locked. There are several reasons why an account is locked; for example, it could be locked by the system administrator or because the user has reached the maximum number of login attempts.</p> <p>Users can be automatically suspended due to multiple concurrent password failures. In that case:</p> <ul style="list-style-type: none"> ▪ Users are automatically suspended for a duration of 30 minutes. ▪ The Default Admin account (cloudadmin@<tenant>) can also be suspended for the same reason; however, the automatic suspension only lasts 5 minutes. ▪ If additional login attempts are made with the wrong password, the suspension time is extended. <p>Automatic suspension ends when the user logs in successfully.</p> <p>The Users tab continues to show the Suspended status until the user logs in successfully.</p>

Account

In the **Account** section, click **Edit** to modify the attribute fields or to upload a profile image.

- **Display name:** The name visible to users once they are logged in to the platform.
- **Username:** The name used to log in to the platform. Users log in with <Login Name>@<domain>. For example, jsmith@acme or jsmith@acme.com.

Users and Groups

- Overview
- Groups
- Roles
- MFA redirection
- Additional attributes

Account

Display name

Username

Email address

Mobile phone

—

Office phone

—

Home phone

—


Description

—

Manager

Unassigned

Profile photo



Advanced Settings

In this section, administrators can set the user's membership type to *Employee* or *Vendor*.

Advanced Settings

Membership type

Employee

Employee

Vendor

Password never expires

☐

Require password change at next login

☐

Is a service user

☐




Account is disabled

☐

Account is locked

☐

Option	Description
Membership type	Employee or Vendor

Option	Description
Password never expires	<p>Overrides the default "Maximum password age" identity policy setting. Regardless of the "Maximum password age" setting, the password for this account never expires.</p> <p> Note: This setting and the "Require password change at next login" setting depend on each other. If you select one, the other is reset.</p>
Require password change at next login	<p>Forces users to create a new password the next time they log in. The user is subject to any password reset policy controls and settings you have enabled. This setting is reset as soon as the user logs in and creates a new password.</p> <p> Note: This setting and the "Password never expires" setting depend on each other. If you select one, the other is reset.</p>
Account is disabled	The account has been disabled.
Account is locked	<p>Locks the user's account. When locked, users are prevented from further access to Delinea Platform services, but they are not locked out entirely in their directory service. This setting can be enabled either manually or automatically through an identity policy. To configure the policy, navigate to the applicable policy. Under Password Setting, set Maximum consecutive bad password attempts allowed.</p> <p> Note: The Default Admin account (cloudadmin@< tenant >) cannot be manually locked. For this account, the option is unavailable.</p>

Secret Server Details

The following user types are available:

- **Hybrid** users have direct access to both the Delinea Platform and Secret Server. Passwords are not synchronized between the platform and Secret Server. Users must reset their passwords independently in platform and Secret Server.

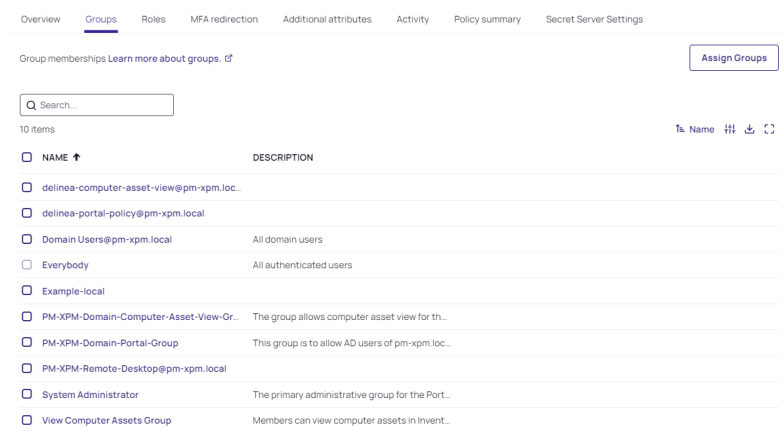
Users and Groups

- **Native** users can only log in through the platform, but not through Secret Server. They cannot authenticate directly with Secret Server.
- **None** means that the user is a Secret Server user only, and is not associated with a platform account.

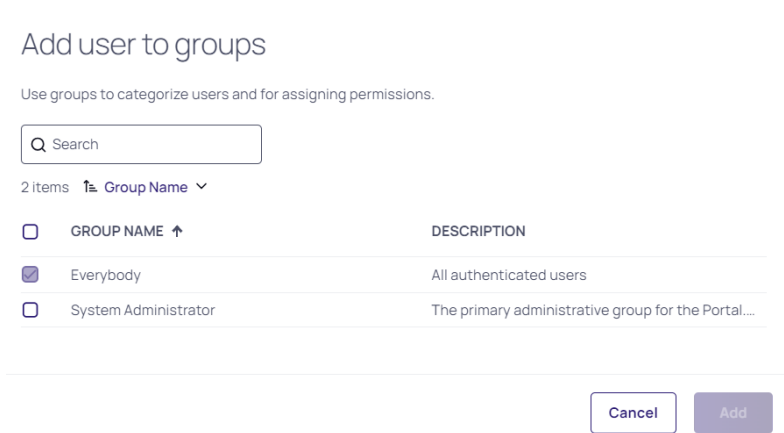
Groups Tab

An administrator can manage group membership from the individual User view as described here, or from the Groups view. See [Managing Groups](#) and [Troubleshooting Federated Group Mapping](#) for more information. To map federated user groups to platform groups, see [Mapping Federated Groups](#). Also see [Mapping Federated Users](#).


1. Click the **Groups** tab to see a list of groups a user belongs to.

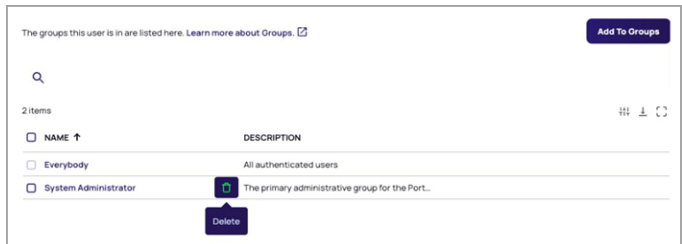


2. To add a user to a group, click **Assign Groups**.
3. Select one or more groups.
4. Click **Add** to add the user to the selected groups.



5. To remove a user from a group, hover your cursor in the group row, near the right end of the **Name** column, and click the trash icon that appears.

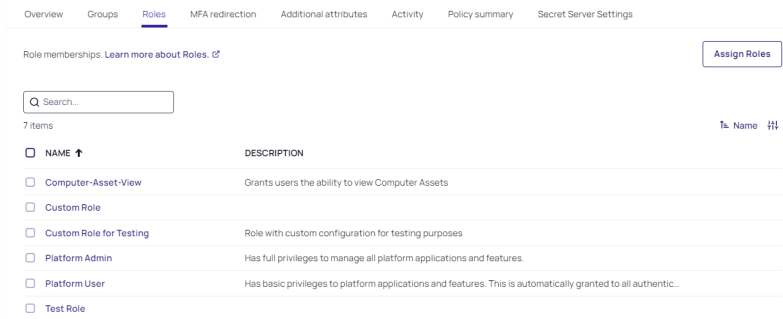
 **Note:** The Everybody group cannot be removed if a user is not a service user.




Roles Tab

An administrator can use the Roles tab to view and manage which roles are assigned to a user.

1. Click the **Roles** tab, which displays the roles the user has been assigned to.



2. Click **Edit** to add or remove role assignments for the user.

 **Important:** It is not considered a best practice to assign a role directly to a user. We strongly recommend assigning a role (with its associated permissions) to a group, then adding the user to the group, at which point the user inherits the role and its permissions by virtue of their membership in the group.

For more detailed information about managing user roles, see "Roles and Permissions" on page 203.

MFA Redirection Tab

Multi-Factor Authentication (MFA) redirection enables users to perform MFA on behalf of any chosen user. This means the user that is logging in can be configured to perform MFA as the redirect user and receive an identity token for the original login user after they successfully log in. Once configured, the MFA redirection is handled automatically.

To explain how redirection works, consider the following two users:

- Original login user: The user who is actively trying to log in.
- Redirect user: The user who has MFA set up. Login attempts are redirected to this user to answer any MFA challenges.

The redirect user performs MFA on behalf of the original login user. Any MFA mechanism that is used, such as email, text, Mobile Authenticator, and so on, is completed by the redirect user. The procedure is as follows:

Users and Groups

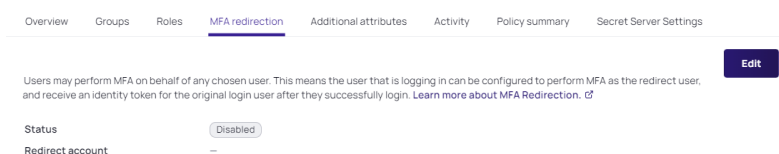
1. The original user attempts to log in with their username.
2. The details for the original login user are retrieved from the Delinea Platform.
3. The redirect user receives MFA challenges for the redirect user's account.
4. When authentication is successful, an identity token/cookie is provided to the original login user.

Typical MFA Redirection Use Cases

MFA redirection is typically used when the original user has no attributes configured, and therefore cannot satisfy any MFA challenge. When the original user is challenged for additional authentication, the MFA redirection feature can be configured so the redirect user's MFA challenges (who has the required mechanisms configured) are used.

Configure MFA Redirection

1. Click the **MFA Redirection** tab. This tab indicates whether MFA redirection is enabled and, if so, the name of the redirect account.



2. Click **Edit**.
3. Select the **Enable redirect of Multi-Factor Authentication to a different user account** checkbox.
4. Click **Select** and select the account you want to use for the MFA redirection.



Note: If you select the same user you're currently editing, an error occurs: *Cannot redirect MFA to the same user.*

5. Click **Save**.

Additional Attributes Tab

The Delinea Platform provides default user attributes, but you can add user attributes with custom values for Active Directory and Delinea Directory users. These added attributes can be useful as valid targets of MFA; for example, as an alternate email or phone number. The added attributes are stored on the Delinea Platform only. They are not copied to Active Directory.

To make additional attributes available for login authentication rules and SAML user authentication, you must first add them here.

1. Click the **Additional attributes** tab.
2. Click **Add Attributes**.

Users and Groups

Configuration

Directory Service

Additional Attributes

Use these settings to extend attributes for users. [Learn more about Additional Attributes.](#) [Add Attributes](#)

2 items

NAME ↑

TYPE

DESCRIPTION

employee_number

Number

employee_status

True/False

3. **Name:** Enter a descriptive name for the attribute. The name can contain only letters, numbers, and underscores. It must start with a letter, and must include at least one underscore. For example: employee_status
4. **Attribute value:** Select the attribute value from the dropdown list.

Add Attribute

Name *

employee_number

Type *

Number

Number

Number (Decimal)

Text

True/False

Date Time

Description

Cancel

Save

Attribute Value	Description
Number	Allow whole numbers
Number (decimal)	Allow numbers with decimals
Text	Allow any string
True/False	Display a dropdown list for the attribute value
Date Time	Display a date and time picker for the attribute value

5. **Description:** Enter a description for the attribute (optional) .
6. Click **Save**.

Activity Tab

The Activity tab lists each of the user's activities (events) on the platform, including the following:

Users and Groups

- Login
- Logout
- Security Question Set
- Password Change
- Password Change Failed
- AD Password Change
- AD Password Change Failed

For each activity, the following information is displayed:

- Date/Time
- Event name
- Status (Success or Failed)
- Browser
- IP Address
- Operating System

Policy Summary Tab

The **Policy Summary** tab displays all information about existing policies currently associated with a specific user. The page does not provide editing capabilities, because all of these policies are managed elsewhere.

Users and Groups

Overview	Groups	Roles	MFA redirection	Additional attributes	Activity	Policy summary	Secret Server Settings
----------	--------	-------	-----------------	-----------------------	----------	----------------	------------------------

The policy summary displays all information about existing policies currently associated with a specific user. [Learn more about policies](#) 

Services

Default Profile

Policy settings	Value	Policy name
Enable authentication policy controls	Yes	local policy
Default authentication profile	local profile	local policy

Browser Session Parameters

Policy settings	Value	Policy name
User idle timeout (Minutes)	15	local policy
Allow the 'Keep me logged in' checkbox option at login (session spans browser sessions)	No	local policy
Session length (Hours)	12	local policy

Delinea Mobile Application Session Parameters

Policy settings	Value	Policy name
Session length (Days)	14	local policy

Other Settings

Policy settings	Value	Policy name
Allow IWA connections (bypasses authentication rules and default profile)	No	local policy
Set identity cookie for IWA connections	No	local policy
IWA connections satisfy all MFA mechanisms	No	local policy
Allow users without a valid authentication factor to log in	No	local policy
Apply additional authentication rules to federated users	No	local policy
Platform login via federation satisfies all MFA mechanisms	Yes	local policy
Allow additional authentication from same device	Yes	local policy
Continue with additional challenges after failed challenge	No	local policy
Do not send challenge request when previous challenge response failed	No	local policy
Remember and suggest last used authentication factor	No	local policy

User security

Password Reset

Policy settings	Value	Policy name
Account self-service controls	Yes	Default Policy
Enable password reset	Yes	Default Policy
Allow for Active Directory users	No	Default Policy
Only allow from browsers with identity cookie	No	Default Policy
User must log in after successful password reset	No	Default Policy
Password reset authentication profile	Default Password Reset Profile	Default Policy

Account Unlock

Policy settings	Value	Policy name
Enable account unlock	No	Default Policy

Additional Policy Parameters

Policy settings	Value	Policy name
Maximum password resets allowed during the capture window	10	Default Policy
Capture window for password resets (default 60 minutes)	60	Default Policy

Password Settings

Display Requirements

Policy settings	Value	Policy name
Show password complexity requirements when entering a new password (default no)	Yes	Default Policy

Capture Settings

Policy settings	Value	Policy name
Maximum consecutive bad password attempts allowed within window (default Off)	5	Default Policy

OATH OTP

OATH OTP integration

Policy settings	Value	Policy name
Enable OATH OTP integration	Yes	PM-XPM-Domain-Portal-Login

Authentication Settings

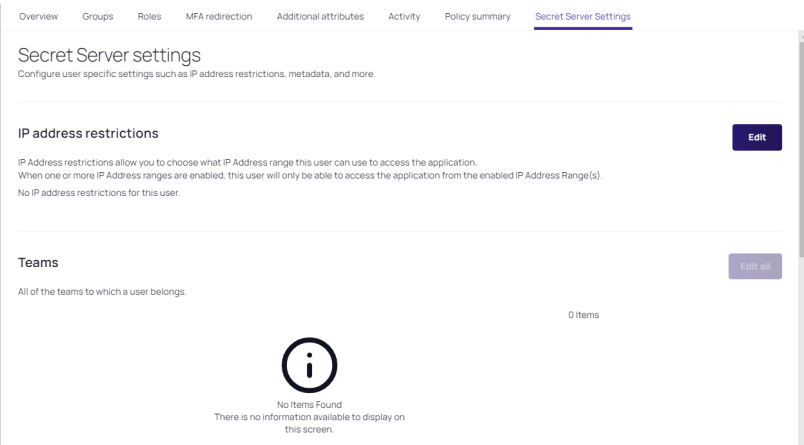
Enable users to enroll FIDO2 authenticators

Policy settings	Value	Policy name
Enabled	Yes	PM-XPM-Domain-Portal-Login
Require users to configure a FIDO2 security key at sign in	No	PM-XPM-Domain-Portal-Login
FIDO2 security key display name	FIDO2	PM-XPM-Domain-Portal-Login

Enable users to configure an OATH OTP client (requires enabling OATH OTP

Secret Server Settings Tab

The Secret Server Settings tab displays the user's settings for Secret Server.



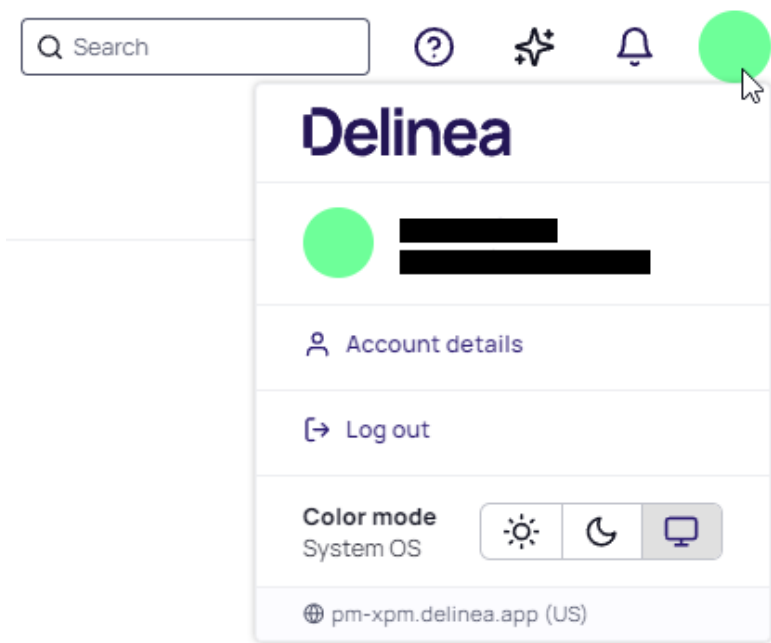
Click **Edit** next to IP address restrictions to add, remove, or modify the user's IP restrictions.

Click **Edit** next to Teams to add, remove, or modify the user's teams.

Managing Your User Profile

The following procedure describes how a user can view and edit their user profile settings.

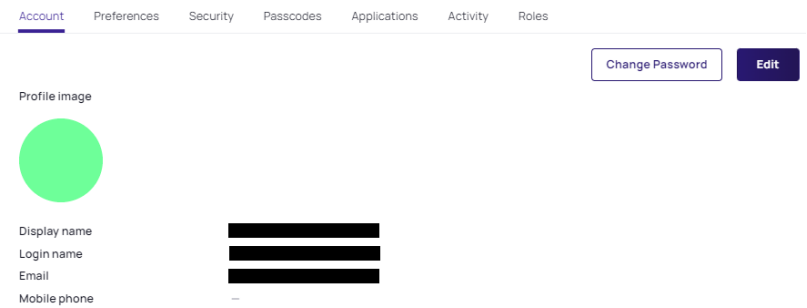
1. Find your user icon at the top right corner of the Delinea Platform interface. By default, the icon is a circle with the user's first and last initials.
2. Click the user icon to open the user profile card.



3. Click **Account Details**. Your user page opens to the Account tab.

Account

The Account tab displays your profile image if you've chosen one, plus your Display name, Login name, Email, and Mobile phone.



To change your password, click **Change Password**.

- 1. To edit your account information click **Edit**. You can edit your Display name, Login name, Email, and Mobile phone information, unless your organization controls them.
- 2. To choose a head shot or other image for your profile, click **Upload Image**. The image will then be used for your user icon.

Users and Groups

Account

Preferences

Security

Passcodes

Applications

Activity

Roles

Profile image

Upload Image

Display name *

Login name *

Email *

Mobile phone

Cancel

Save

Preferences

The Preferences tab displays your editable preferences for the Interface, Email settings, and Launcher settings.

Account

Preferences

Security

Passcodes

Applications

Activity

Roles

Interface

Language

English (English)

Time zone

The time zone that will be used for times when receiving communications such as Email or Slack.

System Default

Time format

System Default

Date format

System Default

Theme

System

Email settings

Users are able to choose what you want to be notified about, based on Secret events. Enabling these email notifications will apply to all Secrets that you have "View" permissions for. For basic users this includes all Secrets within your Personal Folders and often other Secrets that you manage or create. If you do not receive email notifications for certain secrets, ask your administrator about your permission settings for that Secret.

Send email when dependencies fail to update

Send email when secrets are changed

Send email when heartbeat fails for secrets

Send email when secrets are viewed

Launcher settings

Tailor your launchers to fit your workstation needs. These settings will apply to all launchers you use where applicable.

Connect to console

Allow access to printers

Allow access to drives

Allow access to clipboard

Allow access to smart cards

Use Custom Window Size

Email Settings

Under Email settings, you can choose what you want to be notified about, based on Secret events. Enabling these email notifications will apply to all Secrets that you have "View" permissions for, including all secrets in your personal folders and other secrets you created or manage. If you don't receive email notifications you want to receive for a specific secret, ask your platform administrator to review your permissions for that secret.

Launcher Settings

Under Launcher settings, you can tailor settings to fit your workstation needs for all launchers you use.

Security tab

The **Security** tab displays the verification (log in) mechanisms you have configured as well as available optional mechanisms that you can optionally configure. To configure an optional mechanism, click the mechanism card.

Account

Preferences

Security

Passcodes

Applications

Activity

Roles

Configure these verification mechanisms to ensure accurate identity validation.

Configured

Password

Last configured 3/3/24

Optional

Security questions

Click to configure

Optional

Fido2

Click to configure

Optional

On-device authenticator

Click to configure

Passcodes

The Passcodes tab enables you to strengthen your platform login security on the platform by manually enrolling your OATH tokens. The Delinea Platform supports any authenticator app that supports the OATH TOTP standard.

- 1. Click **Create Passcode**. The Create passcode dialog opens.
- 2. Complete the **Issuer** field
- 3. Complete the **Account name** field.
- 4. Enter the OATH parameters from your OATH application/provider.

Create passcode

Follow instructions from the issuer to configure required fields.

Issuer *

Account name *

Secret key *

Min. 2 chars. Base32 encoded.

Key algorithm *

SHA1

OTP digits *

6

Period (Seconds) *

30

Cancel

Save

Secret key, Key algorithm, OTP digits, and Period


The Secret key, Key algorithm, OTP digits, and Period data are specific to the OATH application being manually set up. Users typically scan a QR code in their app to complete these fields. Only an administrator doing a bulk setup would manually enter values in these fields.

Applications

The Applications tab presents you with options to download other Delinea applications.


[Account](#) [Preferences](#) [Security](#) [Passcodes](#) [Applications](#) [Activity](#) [Roles](#)

Download, register, and manage Delinea mobile applications for your user.

**Delinea Mobile**


Access secrets and passcodes from your mobile device.

[Get App](#)

**Authenticator**

Satisfy login and step-up MFA requests from your mobile device.

[Get App](#)

 **Note:** Due to essential backend migration activities for the Delinea Authenticator app, some customers may observe multiple entries for the Delinea Mobile app within the Applications tab of their User Profile. Impacted customers are advised to 'unregister' the older entry to ensure only the updated record is displayed. This action is expected to have no impact on user functionality.

Activity

The Activity tab displays all your platform activities and events, including log ins, log outs, security question set, password change, and AD password change. For each activity, the page displays the status (success or failure), the date and time, and the browser, IP address, and OS used.

[Account](#) [Preferences](#) [Security](#) [Passcodes](#) [Applications](#) [Activity](#) [Roles](#)

Below is a summary of recent activity associated with your profile. [Learn more about Activity](#)

All statuses ▾

All events ▾

- ☒ All events
- ☐ Login
- ☐ Logout
- ☐ Security question set
- ☐ Password change
- ☐ Password change failed
- ☐ AD password change
- ☐ AD password change failed

20 items

DATE/TIME ▾	EVENT	STATUS	BROWSER	ADDRESS	OS
10/1/24, 9:53 AM	Login	Success		118.10.212	Windows (10)
9/30/24, 4:51 PM	Logout	Success		118.10.212	Windows (10)
9/30/24, 4:18 PM	Login	Success		118.10.212	Windows (10)
9/30/24, 4:17 PM	Logout	Success		118.10.212	Windows (10)
9/30/24, 3:55 PM	Login	Success		118.10.212	Windows (10)
9/30/24, 2:54 PM	Login	Success	Chrome (Chrome (129.0.0.0))	98.118.10.212	Windows (10)
9/30/24, 2:43 PM	Logout	Success	Chrome (Chrome (129.0.0.0))	98.118.10.212	Windows (10)

Roles

The Roles tab displays the roles that have been assigned to you, typically through your group memberships.

[Account](#) [Preferences](#) [Security](#) [Passcodes](#) [Applications](#) [Activity](#) [Roles](#)

Your assigned roles. Select a role to see its permissions. [Learn more about Roles.](#)

9 items

NAME ↑	DESCRIPTION
Custom Role for Testing	Role with custom configuration for testing purposes
Platform Admin	Has full privileges to manage all platform applications and features.
Platform User	Has basic privileges to platform applications and features. This is automatically granted to all authenticated users.

Click the role name. The role page opens to the Permissions tab, which displays the permissions granted through that role.

Platform User

[Overview](#) [Permissions](#) [Members](#)

4 items

TITLE ↑	NAME	DESCRIPTION
Launch PRA Session	delinea.platform/remotefaccess/session/launch	Can Launch a Privileged Remote Access session
Read Own Audit events	delinea.platform/audit/event/own/read	Allows a user to read their own administrative and privileged activity events
View Own Session Recordings	delinea.platform/audit/sessionrecording/own/read	Allows a user to open and view their personal session recordings
View Secrets	delinea.platform/remotefaccess/secret/read	Can View Secrets to launch Privileged Remote Access sessions

Managing Groups


This page explains how to manage groups.

Predefined Groups

The Delinea Platform has two predefined groups:

- **Everybody:** All platform users belong to the Everybody group. Through that group membership they inherit the Platform User role, with permissions to log in to the Delinea Platform, access their secrets, launch PRA sessions, and view their own session recordings. The Everybody group cannot be renamed or deleted.
- **System Administrator:** Platform users who belong to the System Administrator group inherit the Platform Admin role, with all administrative permissions. When the Delinea Platform is first installed, the user account that is created automatically belongs to the System Administrator group. The System Administrator group cannot be renamed or deleted.

Types of Groups

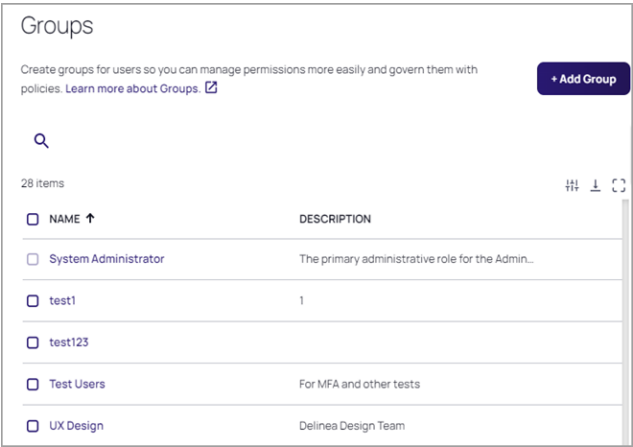
 **Note:** The platform supports the following types of groups: global AD security groups, universal AD security groups, Entra ID security groups, and user attributes/claims named **groups**.

It does not support domain local groups. It also does not support distribution lists. A **distribution list**, sometimes inaccurately called a *distribution group*, is used to send email to users specified on the list. But on any access control system including the Delinea Platform, groups are used for access control. A distribution list cannot be used for access control because it cannot be listed in discretionary access control lists (DACLS). A distribution list has no index, so you can't query it to determine if a user (trying to access something) is or is not on the list, rendering the distribution list useless for purposes of controlling access.

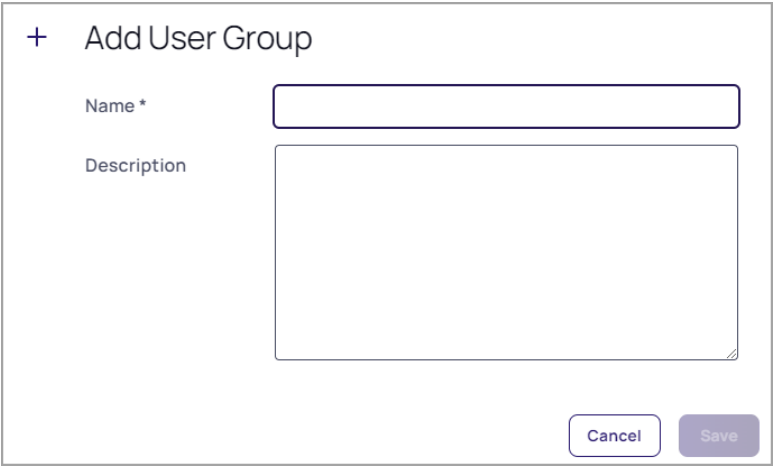
For more information on groups, roles, and permissions, see "Roles and Permissions" on page 203.

Adding a Group

1. Click **Access** from the left navigation, then select **Groups**.



2. Click **Add Group**.



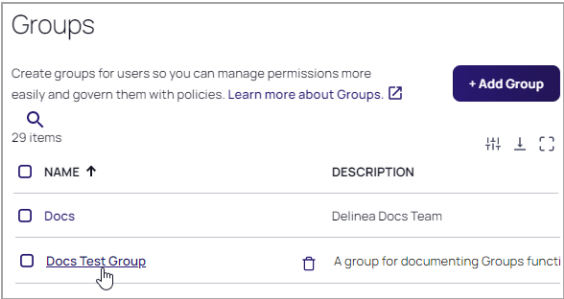
Users and Groups

- 3. Click **Save**.
- 4. On the Add group page, enter a group **Name** and **Description**.
- 5. Click **Save**.

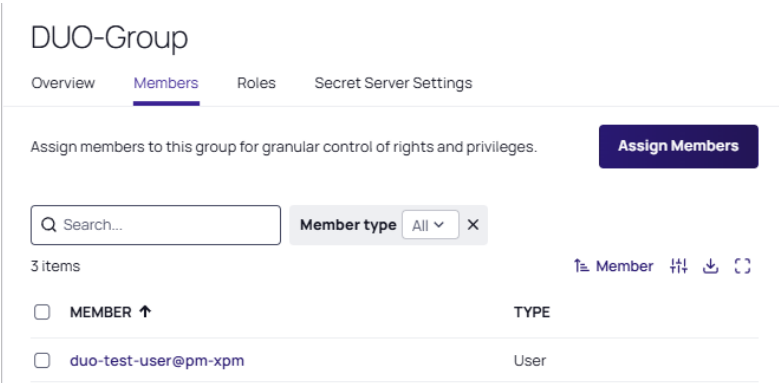
Adding Users to a Group

You can add several types of members to a group, including users, directory groups such as AD, and Delinea groups. To add a member to a group, follow these steps:

- 1. Click **Access** from the left navigation menu, then select **Groups**.
- 2. On the Groups page, click a group.



- 3. On the specific group page, click the **Members** tab.



- 4. Click **Assign Members**.

Users and Groups

5. On the **Assign members** page, search for and select each user you want to add, then click **Add**.

Assign members

Member typeUsers X

TypeUsers X

Directory sourceDelinea Directory X

113 items 1% Username

<input type="checkbox"/> USERNAME ↑	DISPLAY NAME	EMAIL ADDRESS	DIRECTORY SOURCE
<input type="checkbox"/> local2@pm-xpm	Local 2	a@delinea.com	Delinea Directory
<input type="checkbox"/> local@pm-xpm	Local User (Everybody)	a@delinea.com	Delinea Directory
<input type="checkbox"/> localuser@pm-xpm	Local User (Non-Admin)	a@delinea.com	Delinea Directory
<input type="checkbox"/> localvendor@pm-xpm	LocalVendor	a@delinea.com	Delinea Directory

Cancel

Add

User Directory Service Configuration

- Click **Settings** from the left navigation, then select **Directory services**.
- Select the checkbox next to a directory service you want to use or remove. Actions available for a selected directory service vary:
 - Delinea and Federated directory are read only (no actions).
 - Active directory can only be moved (no remove).
 - Other directory types can be removed.

A dialog appears with options that include one or more of the following, depending on the type of directory or directories you selected: **Clear Selected**, **Move Down**, **Move Up**, or **Remove Selected**.

Configuration

Directory Service Additional Attributes

Use these settings to add and order directory services. Directory services are listed in order of lookup. Drag directory service to specify lookup order.

5 items

TYPE

NAME

☐ Delinea Directory

Delinea Directory

☒ Active Directory

Active Directory: AD-WEBST.COM

☐ Active Directory

Active Directory: cloudev.test

☐ Active Directory

Active Directory: testparent.thycotic.com

☐ Federated Directory

Federated Directory Service

X Clear Selected

Move Down

Move Up

Additional Attributes

- 1. On the Configuration page, click the **Additional Attributes** tab.

Configuration

Directory Service

Additional Attributes

Use these settings to extend attributes for users

Learn more about Additional Attributes. [↗](#)

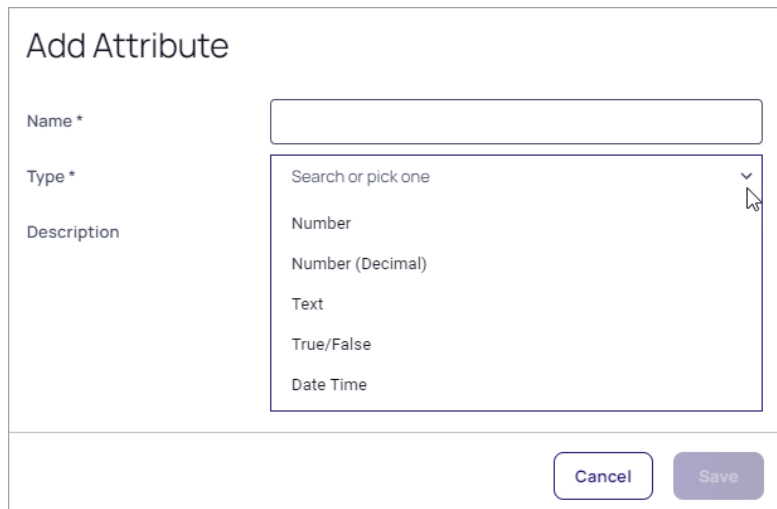
Add Attributes

🔍

6 items

<input type="checkbox"/> NAME ↑	TYPE	DESCRIPTION
<input type="checkbox"/> points_attr	Number	asdasfaw
<input type="checkbox"/> ported_attr	True/False	Ported from old
<input type="checkbox"/> test_bool	True/False	
<input type="checkbox"/> test_datetime	Date Time	
<input type="checkbox"/> test_text	Text	

- 2. Click **Add Attributes**.
- 3. On the Add Attributes page, enter a name in the **Name** field. The name can contain only letters, numbers, and underscores. It must begin with a letter and contain at least one underscore.



Add Attribute

Name *

Type *

Search or pick one
Number
Number (Decimal)
Text
True/False
Date Time

Description

4. In the **Type** field, search for a type or click the dropdown arrow and pick one of the following:

- Number
- Number (Decimal)
- Text
- True/False
- Data Time

5. Click **Save**. A message appears: **Your Attribute has been Added Successfully**.



Note: On the platform, user roles and their associated permissions are assigned to users through the users' memberships in platform groups, including platform groups mapped to federated groups (see [Mapping Federated Groups](#)). For more information on groups, roles, and permissions, see [Understanding Roles and Permissions](#).

For related content, see the following:

- [Managing Users and Groups](#)
- [Managing User Accounts](#)
- [Managing Your User Profile](#)

External Directory Group Allowlist



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

External directory groups are groups that are managed by an external identity provider (IdP), such as Microsoft Entra ID or Active Directory. These groups are not created or maintained directly within the Delinea Platform. By default, when you integrate with Entra ID, all security groups from your directory are browsable within the platform. However, if you need more control, platform administrators can choose to limit which external groups are available.

To do this, simply add the desired groups to the platform's **External Groups** list. Once this list is defined, *only the specified groups will be available* when managing roles, applying identity policies, or sharing secrets. This global change allows you to ensure that only relevant groups are used across your tenant, enhancing usability, security, and administrative control.

Create or Update an External Group List

1. On the Delinea Platform, navigate to **Access > Groups**.
2. Select the **External groups** tab.
3. Click **Set external group availability**.
4. Select the **Directory source** to start browsing for groups.
5. Select the desired groups for use on the Delinea Platform.
6. Click **Add**.

The selected groups now appear in the External Groups list. Only these groups will be available in the platform for assigning roles, applying identity policies, and managing secret permissions. To restore the default experience—where all groups from all external directories are browsable—simply clear the external group list.

Delete Groups from the External Group List

1. On the Delinea Platform, navigate to **Access > Groups**.
2. Select the **External groups** tab.
3. Select the groups to be removed by selecting the checkbox next to the group.
4. Click **Remove**.
5. At the confirmation dialog click **Remove**.

The selected groups are now removed from the External Groups list. Removing all groups restores the default browsing experience.

Roles and Permissions

Delinea Platform's role-based access control system precisely manages resource access, so you can authorize users with the exact permissions they need.

Unified Roles and Permissions in Secret Server and Platform

For new customers of Delinea Platform and Secret Server, all roles and permissions are centrally managed within the platform.

As of November 8, 2023, all newly provisioned customers on Delinea Platform experience a unified roles and permissions system. All Secret Server roles and permissions are managed centrally within Delinea Platform.

Roles and Permissions

- Delinea Platform serves as the authoritative source for role permissions within Secret Server. All Secret Server permissions are displayed under platform permissions.
- Secret Server user, group, and role management are no longer accessible under Secret Server Settings.



Note: Access to Secret Server requires the *Secret Server Access* permission.

Built-in Roles

The platform provides two built-in roles, which cannot be disabled:

- **Platform User:** All platform users belong to the Everybody group, and inherit the Platform User role through their membership in that group. The Everybody group is removable; however, the Platform User role provides basic permissions for a user to log in to the platform, launch PRA sessions, access their own secrets, and view their own session recordings.
- **Platform Admin:** Platform users who belong to the System Administrator group inherit the Platform Admin role through their membership in that group. The Platform Admin role provides all permissions on the platform.

Custom Roles

The platform also supports the creation, editing, and deletion of custom roles. Those topics are covered later in this page.

Permissions

Platform permissions are made available for assignment to Roles according to the services available in your platform environment.

Users, Groups, Roles, and Permissions

On the platform, user roles and their associated permissions are assigned to users through the users' memberships in platform groups, including platform groups mapped to federated groups. To understand the relationships between users, groups, roles, and permissions, review the following points:

- A permission can be assigned to one or more roles, but cannot be assigned directly to a group or a user.
- A role can be assigned to one or more groups, and a group can be assigned to one or more users.
- A user inherits one or more roles, along with each role's permissions, through the group or groups the user is assigned to.



Note: Although the platform permits you to assign a role directly to a user, the best practice is to assign a role to a user only through the groups the user is assigned to.

Edit Role Permissions

To edit an existing role:

Roles and Permissions

1. Click **Access** from the left navigation menu, then select **Roles**.

Q Search the Delinea Platform

?

🔔

🔄

●

Roles

Q Search...

All Types ▾

Create Role

7 Items

IF Type 🗑️ ⬇️ ↺

ROLE NAME	TYPE ↓	DESCRIPTION	STATUS
Platform User	Built in	Has basic privileges to platform ...	Enabled
Platform Admin	Built in	Has full privileges to manage all ...	Enabled
Platform Vault User	Custom		Enabled
Custom Role	Custom		Enabled
Computer-Asset-View	Custom	Grants users the ability to view ...	Enabled

2. Click the name of one of the roles displayed. The role page opens to the Overview tab.

Roles >

Q Search the Delinea Platform

?

🔔

🔄

●

Custom Role

Delete Role

Overview Permissions Members

Use roles to group permissions together and assign them to Users and Groups.

Edit

Status

Enabled

Role Name

Custom Role

Type

Custom

Role Description

None

3. Click the **Permissions** tab. All permissions assigned to the role are listed on the tab.

Roles >

Q Search the Delinea Platform

?

🔔

🔄

●

Custom Role

Delete Role

Overview Permissions Members

Q Search...

All ▾

Add Permissions

91 Items

🔍 Title 🗑️ ⬇️ ↺

<input type="checkbox"/> TITLE ↑	NAME	DESCRIPTION
<input type="checkbox"/> Ability to download files from a target sy...	delinea.platform/remotefiletransfer/...	This permission enables the user to dow...
<input type="checkbox"/> Ability to upload files to a target system	delinea.platform/remotefiletransfer/...	This permission enables the user to uplo...
<input type="checkbox"/> Activate RAS Engine	delinea.platform/administration/remote...	Can activate Remote Access OnPrem en...
<input type="checkbox"/> Add Engine	delinea.enginepool/engine/create	Ability to create a new engine.
<input type="checkbox"/> Add Federation Profile	delinea.platform/administration/federat...	Add a federation profile
<input type="checkbox"/> Add Group Role Assignment	delinea.platform/administration/groups...	Can assign groups to roles.
<input type="checkbox"/> Add RAS Engine	delinea.platform/administration/remote...	Can add Remote Access OnPrem engine

Roles and Permissions

4. To add a permission to the role, click **Add Permission**. The Add Permissions dialog pops up.

Add Permissions

Q Search...

All ▾

91 items

Title

<input type="checkbox"/> TITLE ↑	NAME	DESCRIPTION
<input type="checkbox"/> Ability to download files from a target syst...	delinea.platform/remotearchess/filetransf...	This permission enables the user to downl...
<input type="checkbox"/> Ability to upload files to a target system	delinea.platform/remotearchess/filetransf...	This permission enables the user to uploa...
<input type="checkbox"/> Activate RAS Engine	delinea.platform/administration/remotearc...	Can activate Remote Access OnPrem engi...
<input type="checkbox"/> Add Engine	delinea.enginepool/engine/create	Ability to create a new engine.
<input type="checkbox"/> Add Federation Profile	delinea.platform/administration/federatio...	Add a federation profile
<input type="checkbox"/> Add Group Role Assignment	delinea.platform/administration/groups/ro...	Can assign groups to roles.
<input type="checkbox"/> Add RAS Engine	delinea.platform/administration/remotearc...	Can add Remote Access OnPrem engine
<input type="checkbox"/> Add Roles	delinea.platform/administration/roles/cre...	Can add roles.
<input type="checkbox"/> Add Secret Server Templates	delinea.platform/administration/remotearc...	Can add Secret Server templates
<input type="checkbox"/> Add User Role Assignments	delinea.platform/administration/users/rol...	Can assign users to roles.

Cancel

Assign

5. Select the box next to each permission you would like to add to the role.

Add Permissions

<input checked="" type="checkbox"/>	Launch RAS Session	delinea.platform/remotearchess/session/l...	Can Launch a Remote Access session
<input checked="" type="checkbox"/>	List Engines	delinea.enginepool/engine/list	Ability to view summary information about ...
<input checked="" type="checkbox"/>	List Registration Codes	delinea.registration/registrationcode/list	The user can view summary information ab...
<input type="checkbox"/>	List Registrations	delinea.registration/registrationcode/regi...	The user can view summary information ab...
<input type="checkbox"/>	List Sites	delinea.enginepool/site/list	Ability to view summary information about ...
<input type="checkbox"/>	List Workload Definitions	delinea.registration/workloaddefinition/list	The user can view summary information ab...
<input type="checkbox"/>	Manage Behavioral Analytics	delinea.platform/analytics/settings/mana...	Can manage Behavioral Analytics settings.
<input type="checkbox"/>	Manage Identity settings	delinea.platform/identity/admin/manage	Can manage all Identity related settings s...
<input type="checkbox"/>	Manage Webhooks	delinea.platform/webhooks/manage	Can manage all webhooks
<input type="checkbox"/>	Read Another Users Profile Settings	delinea.platform/userprofile/manage/read	Ability to read other users profile settings. ...
<input type="checkbox"/>	Read Audit events	delinea.platform/audit/event/read	Allows a user to read all administrative and...
<input type="checkbox"/>	Read Federation Profile	delinea.platform/administration/federatio...	Read federation profiles
<input type="checkbox"/>	Read Own Audit events	delinea.platform/audit/event/own/read	Allows a user to read their own administrat...

3 Permissions selected

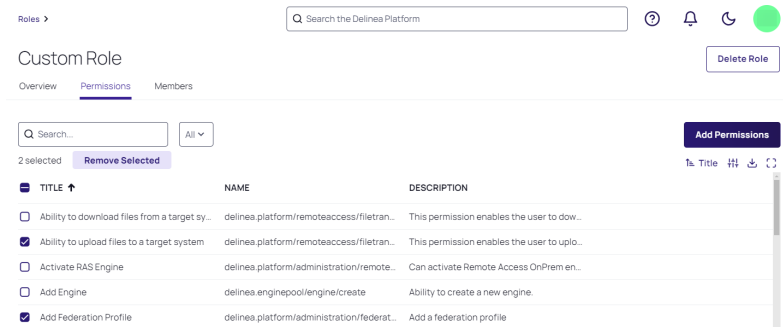
Cancel

Assign

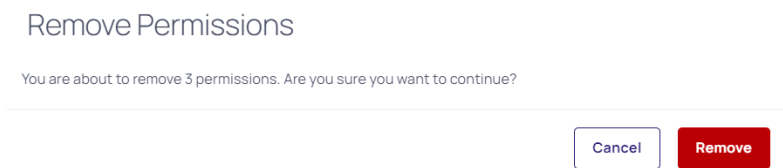
6. Click **Assign**.

Roles and Permissions

7. To remove one or more permissions assigned to a role, select the box next to each permission you would like to remove, then click **Remove Selected**.

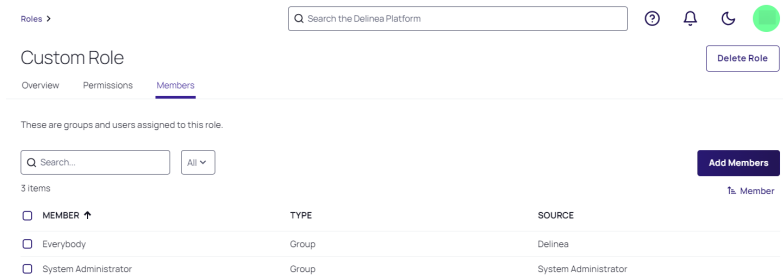


8. Click **Remove** from the pop-up banner to confirm that you want to remove the permission(s).



Edit Role Members (Groups)

1. Click the **Members** tab.
2. To add members (groups) to the role, click **Add Members**.



3. The Add Members dialog pops up.

Roles and Permissions

Add Members

Groups ▾

Delinea Directory ▾

3 items

1a Member

<input checked="" type="checkbox"/> MEMBER ↑	TYPE	SOURCE
<input checked="" type="checkbox"/> Example-local	Group	Delinea
<input type="checkbox"/> PM-XPM-Domain-Computer-Asset-View-G...	Group	Delinea
<input type="checkbox"/> PM-XPM-Domain-Portal-Group	Group	Delinea

1 selected

CancelAdd

4. Select the box next to the groups you want to add, then click **Add**.
5. To remove members (groups) from the role, go to the Members tab and select the box next to each group you wish to delete, then click **Remove Selected**.

Roles >

Custom Role

OverviewPermissionsMembers

These are groups and users assigned to this role.

All ▾

2 selected

Remove Selected

Add Members

1a Member

<input checked="" type="checkbox"/> MEMBER ↑	TYPE	SOURCE
<input type="checkbox"/> Everybody	Group	Delinea
<input checked="" type="checkbox"/> Example-local	Group	Example-local
<input type="checkbox"/> System Administrator	Group	System Administrator
<input checked="" type="checkbox"/> View Computer Assets Group	Group	View Computer Assets Group

Delete a Role

1. Click **Access** from the left navigation menu, then select **Roles**.
2. Hover your cursor over the role you wish to delete, then click the trash icon that appears.

Roles

All Types ▾

Create Role

7 items

IF Type

ROLE NAME	TYPE ↓	DESCRIPTION	STATUS
Platform User	Built in	Has basic privileges to platform ...	Enabled
Platform Admin	Built in	Has full privileges to manage all ...	Enabled
Platform Vault User	Custom		Enabled
Test Role	Custom		Enabled

3. Click **Delete** from the confirmation pop-up.

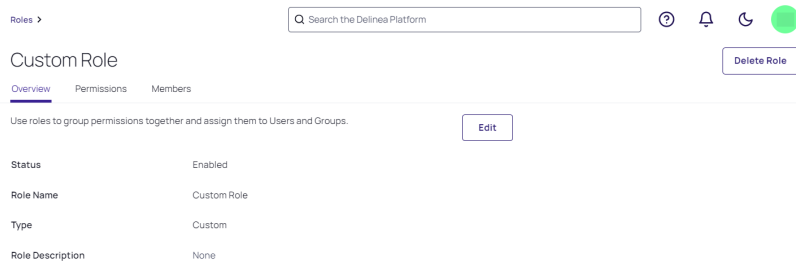
Delete Role

You are about to delete role "Test Role". Are you sure you want to continue?

CancelDelete



Note: You can also delete a role directly from the role's details page by clicking the **Delete** button at the top right of the page.



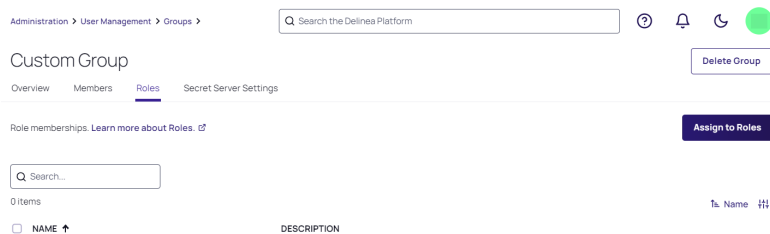
Assign a Group to a Role



Note: The platform supports the following types of groups: global AD security groups, universal AD security groups, Entra ID security groups, and user attributes/claims named **groups**.

It does not support domain local groups. It also does not support distribution lists. A **distribution list**, sometimes inaccurately called a *distribution group*, is used to send email to users specified on the list. But on any access control system including the Delinea Platform, groups are used for access control. A distribution list cannot be used for access control because it cannot be listed in discretionary access control lists (DACLS). A distribution list has no index, so you can't query it to determine if a user (trying to access something) is or is not on the list, rendering the distribution list useless for purposes of controlling access.

1. Click **Access** from the left navigation, then select **Groups**.
2. Select a group you would like to assign to a role.
3. Select the Roles tab, and click **Assign to Role**.



4. Select the role(s) and click **Assign**.

Roles and Permissions

Assign to Roles

7 items

NAME ↑

DESCRIPTION

<input type="checkbox"/>	Computer-Asset-View	Grants users the ability to view Computer Assets
<input checked="" type="checkbox"/>	Custom Role	
<input type="checkbox"/>	Platform Admin	Has full privileges to manage all platform applications and features.
<input checked="" type="checkbox"/>	Platform User	Has basic privileges to platform applications and features. This is a...
<input type="checkbox"/>	Platform Vault User	
<input type="checkbox"/>	Test Role	
<input type="checkbox"/>	test-yang	

2 Roles selected

Cancel

Assign

Create a New Role

1. Click **Access** from the left navigation menu, then select **Roles**.





Roles

Q Search...

All Types ▾

8 items

Create Role

IF Type    

ROLE NAME	TYPE ↓	DESCRIPTION	STATUS
Platform User	Built in	Has basic privileges to platform ...	Enabled
Platform Admin	Built in	Has full privileges to manage all ...	Enabled
Custom Role for Testing	Custom	Role with custom configuration f...	Enabled
Platform Vault User	Custom		Enabled
Test Role	Custom		Enabled

2. Click **Create Role**.
3. To create a new role from scratch, select **Create New Custom Role**. To create a role by cloning an existing role and editing it, select **Clone Existing Role**.

Create Role

Create a new role or clone an existing role. Which will copy an existing role's permissions

Role Type

☒ Create New Custom Role ☐ Clone Existing Role

Role Name

Role Description

Cancel

Save

4. Enter appropriate information in the **Role Name** and **Role Description** fields.
5. Click **Save**.

Roles and Permissions

- Click the **Permissions** tab.
- Click **Add Permissions** to assign appropriate permissions to the role.
 - To search through existing permissions, enter terms into the Search box.
 - To restrict your search results to just one type of permission, make your selection from the **All** dropdown list.

Add Permissions

Q Search...

All ▾

91 items

☐ TITLE ↑

☐ Ability to download files from a tar...

☐ Ability to upload files to a target s...

☐ Activate RAS Engine

☐ Add Engine

☐ Add Federation Profile

☐ Add Group Role Assignment

☐ Add RAS Engine

☐ Add Roles

☐ Add Secret Server Templates

☐ Add User Role Assignments

☒ All

☐ Administration

☐ Behavioral Analytics

☐ Platform Audit

☐ Identity

☐ Marketplace

☐ Remote Access

DESCRIPTION
/remoteaccess/filetransf...
This permission enables the user to downl...
/remoteaccess/filetransf...
This permission enables the user to uploa...
/administration/remotear...
Can activate Remote Access OnPrem engi...
pol/engine/create
Ability to create a new engine.
delinea.platform/administration/federatio...
Add a federation profile
delinea.platform/administration/groups/ro...
Can assign groups to roles.
delinea.platform/administration/remotear...
Can add Remote Access OnPrem engine
delinea.platform/administration/roles/cre...
Can add roles.
delinea.platform/administration/remotear...
Can add Secret Server templates
delinea.platform/administration/users/rol...
Can assign users to roles.

Cancel Assign

- Click **Assign**.

Add Members (Groups) to a Role

- Click the **Members** tab.
- Click **Add Members**.

Add Members

Q Search...

Groups ▾

Delinea Directory ▾

5 items

☒ MEMBER ↑

☐ Everybody

☐ PM-XPM-Domain-Computer-Asset-View-G...

☐ PM-XPM-Domain-Portal-Group

☒ System Administrator

☒ View Computer Assets Group

TYPE	SOURCE
Group	Delinea
Group	Delinea
Group	Delinea
Group	Delinea
Group	Delinea

2 selected

Cancel Add

- To search through existing groups, enter terms in the Search box.
- The first search filter is set to restrict search results to **Groups** by default. Although you can select Users from the dropdown list, adding individual users to a role is not considered a best practice.

Roles and Permissions

- To search across a specific directory (for example, Active Directory), click the Delinea Directory dropdown list and select the desired directory.

3. When you have made your selections, click **Add**.

Platform Permissions

This page provides a reference to the role permissions available in the Delinea Platform.

Miscellaneous Permissions

Permission Name	Description	Permission String
Add Engine	Create a new engine.	delinea.enginepool/engine/create
Administer Analytics	View and edit the settings for analytics.	delinea.analytics/settings/administer
Administer Audit Data Retention	Manage audit data retention, such as editing and running now. This permission does not automatically come with the Administrator role.	delinea.insights/administration/dataretention/administer
Administer Discovery	View and import computers and accounts that are found by Discovery.	delinea.discovery/discovery/administer
Administer Inbox	Administer notification settings for the inbox.	delinea.inbox/inbox/administer
Administer Licenses	View, edit, install, and delete licenses.	delinea.license/administration/licenses/administer
Administer Session Recording Configuration	View and edit session recording settings on the Session Recording tab of Configuration settings. (Formerly also known as Administer Session Recordings.)	delinea.audit/administration/sessionrecording/manage
Approve Registration	Approve a registration.	delinea.registration/registration/approve
Approve Via DUO Push	Approve access requests via Duo push notifications. Administrators do not have this permission by default.	delinea.inbox/duo/requestaccess/approve
Create a Site	Create a new site.	delinea.enginepool/site/create
Create Command Group	Create command groups.	delinea.policy/commandgroups/create
Create Granular Command	Create granular commands.	delinea.policy/commands/create
Create Policy	Create policies.	delinea.policy/policies/create

Roles and Permissions

Permission Name	Description	Permission String
Create Registration Code	Create a registration code.	delinea.registration/registrationcode/create
Delete a Site	Delete a site.	delinea.enginepool/site/delete
Delete Command Group	Delete command groups.	delinea.policy/commandgroups/delete
Delete Engine	Delete an engine.	delinea.enginepool/engine/delete
Delete Granular Command	Delete granular commands.	delinea.policy/commands/delete
Delete Policy	Delete policies.	delinea.policy/policies/delete
Edit Command Group	Edit command groups.	delinea.policy/commandgroups/update
Edit Granular Command	Edit granular commands.	delinea.policy/commands/update
Edit Policy	Edit policies.	delinea.policy/policies/update
Enable Policy	Enable policies.	delinea.policy/policies/enable
Generate a Device Code	Generate a device code.	delinea.registration/devicecode/generate
List Engines	View summary information about all engines.	delinea.enginepool/engine/list
List Registration Codes	View summary information about all registration codes.	delinea.registration/registrationcode/list
List Registrations	View summary information about all registrations for a registration code.	delinea.registration/registrationcode/registration/list
List Sites	See and choose sites through the platform UI, such as in a dropdown list of sites in the PRA setup page. This permission does not grant the ability to view and modify sites through the Engine Management page. For that, the Manage Sites permission is required.	delinea.enginepool/site/list
List Workload Definitions	View summary information about all workload definitions.	delinea.registration/workloaddefinition/list
Manage All Collections	Manage all collections in the tenant.	delinea.platform/collections/manage
Manage Entitlements	Manage entitlement assignments in access.	delinea.platform/access/entitlements/manage

Roles and Permissions

Permission Name	Description	Permission String
Manage Sites	View summary information about all sites and make changes.	delinea.enginepool/site/manage
Manage Webhooks	Manage webhooks.	delinea.platform/webhooks/manage
Read Another Users Profile Settings	Read other users' profile settings (such as the profile image).	delinea.platform/userprofile/manage/read
Register a Workload	Register a Workload with a registration code.	delinea.registration/registrationcode/register
Retrieve a Managed Application Registration	Retrieve a managed application registration.	delinea.registration/registration/managedapplication/retrieve
Retrieve a Registration	Read detailed information (including sensitive information) about individual registrations.	delinea.registration/registration/read
Retrieve Registration Code	Read detailed information (including sensitive information) about individual registration codes.	delinea.registration/registrationcode/read
Retrieve Workload Definition	Read detailed information (including sensitive information) about individual workload definitions.	delinea.registration/workloaddefinition/read
Update a Site	Edit a site.	delinea.enginepool/site/update
Update Another Users Profile Settings	Update other users' profile settings (such as the profile image).	delinea.platform/userprofile/manage/update
Update Engine	Edit an engine.	delinea.enginepool/engine/update
View All Collections	View all collections in the tenant.	delinea.platform/collections/read
View All Computers	The user can view all computers that the user is permitted to access in the tenant.	delinea.assets/computer/view
View Analytics	View, but not edit, settings for analytics.	delinea.analytics/settings/read
View Audit Data Retention	View retained audit data. This permission does not automatically come with the Administrator role.	delinea.insights/administration/dataretention/read
View Command Group	View command groups.	delinea.policy/commandgroups/read

Roles and Permissions

Permission Name	Description	Permission String
View Discovery	View, but not edit, computers and accounts that are found by Discovery.	delinea.discovery/discovery/read
View Engine	Read detailed information about an engine.	delinea.enginepool/engine/read
View Granular Command	View granular commands.	delinea.policy/commands/read
View licenses	View, but not edit, the licenses in the system.	delinea.license/administration/licenses/read
View Policy	View policies.	delinea.policy/policies/read
View Session Recording Configuration	View session recording settings on the Session Recording tab of Configuration settings.	delinea.audit/administration/sessionrecording/read
View Session Recording Comments	Read comments in session recording.	delinea.platform/audit/sessionrecording/comment/read
View Session Recordings	View active launcher sessions.	delinea.audit/sessionrecording/readall
View Site	Read detailed information about a site. (Formerly Retrieve Site.)	delinea.enginepool/site/read

Administration Permissions

Permission Name	Description	Permission String
Activate PRA Engine	Activate Privileged Remote Access engine.	delinea.platform/administration/remotefaccess/engine/activate
Add Federation Profile	Add a federation profile.	delinea.platform/administration/federation/profile/create
Add Group Role Assignment	Assign groups to roles.	delinea.platform/administration/groups/roleassignment/create
Add PRA Engine	Add Privileged Remote Access engine.	delinea.platform/administration/remotefaccess/engine/create
Add Roles	Add roles.	delinea.platform/administration/roles/create
Add Secret Server On Premises Templates	Add Secret Server On Premises templates. (Formerly Add Secret Server Templates.)	delinea.platform/administration/remotefaccess/secrettemplate/create
Add User Role Assignments	Assign users to roles.	delinea.platform/administration/users/roleassignment/create

Roles and Permissions

Permission Name	Description	Permission String
Configure Secret Server On Premises integration	Configure Secret Server On Premises integration.	delinea.platform/administration/remoteaccess/vault/configure
Create PRA Site	Create a new Remote Access site to install engines.	delinea.platform/administration/remoteaccess/site/create
Delete Federation Profile	Delete a federation profile.	delinea.platform/administration/federation/profile/delete
Delete Group Role Assignment	Remove groups from roles.	delinea.platform/administration/groups/roleassignment/delete
Delete PRA Engine	Delete Privileged Remote Access engine.	delinea.platform/administration/remoteaccess/engine/delete
Delete PRA Site	Delete Privileged Remote Access site.	delinea.platform/administration/remoteaccess/site/delete
Delete Roles	Delete roles.	delinea.platform/administration/roles/delete
Delete Secret Server On Premises Templates	Delete Secret Server On Premises templates. (Formerly Delete Secret Server Templates.)	delinea.platform/administration/remoteaccess/secrettemplate/delete
Delete User Role Assignment	Remove users from roles.	delinea.platform/administration/users/roleassignment/delete
Read Federation Profile	Read federation profiles.	delinea.platform/administration/federation/profile/read
Update Federation Profile	Update a federation profile.	delinea.platform/administration/federation/profile/update
Update PRA Engine	Upgrade Privileged Remote Access engine.	delinea.platform/administration/remoteaccess/engine/update
Update PRA Site	Update Privileged Remote Access site.	delinea.platform/administration/remoteaccess/site/update
Update Roles	Modify roles.	delinea.platform/administration/roles/update
Update Tenant Profile	Edit and update any information under the Tenant Profile page. This permission is not additive, so by only having the "Update Tenant Profile" permission, you do not get the ability to also see the data.	delinea.platform/administration/tenantprofile/update

Roles and Permissions

Permission Name	Description	Permission String
View Group Role Assignment	View roles assigned to groups.	delinea.platform/administration/groups/roleassignment/read
View Other User/Group Permissions	Read the permissions of other users and groups.	delinea.platform/administration/haspermission/read
View Permissions	Grants a user permission to view permissions .	delinea.platform/administration/permissions/read
View Platform Groups	View platform groups.	delinea.platform/administration/groups/read
View Platform Users	View platform users.	delinea.platform/administration/users/read
View PRA Engine	View Privileged Remote Access engine.	delinea.platform/administration/remoteaccess/engine/read
View PRA Site	View Privileged Remote Access Site.	delinea.platform/administration/remoteaccess/site/read
View Roles	View roles.	delinea.platform/administration/roles/read
View Tenant Profile	View tenant profile.	delinea.platform/administration/tenantprofile/read
View Secret Server On Premises Integration	View Secret Server On-Premises integration. (Formerly View Secret Server integration.)	delinea.platform/administration/remoteaccess/vault/read
View Secret Server On Premises Templates	View Secret Server On-Premises templates. (Formerly View Secret Server Templates.)	delinea.platform/administration/remoteaccess/secrettemplate/read
View User Role Assignments	View roles assigned to users.	delinea.platform/administration/users/roleassignment/read

Behavioral Analytics Permissions

Permission Name	Description	Permission String
Create Behavioral Analytics Notes	Create behavioral analytics notes.	delinea.platform/analytics/notes/create
Create Behavioral Analytics Settings	Create behavioral analytics settings.	delinea.platform/analytics/settings/create

Roles and Permissions

Permission Name	Description	Permission String
Delete Behavioral Analytics Notes	Delete behavioral analytics notes.	delinea.platform/analytics/notes/delete
Delete Behavioral Analytics Settings	Delete behavioral analytics events.	delinea.platform/analytics/settings/delete
Manage Behavioral Analytics	Manage behavioral analytics settings.	delinea.platform/analytics/settings/manage
Update Behavioral Analytics Alerts	Update behavioral analytics alerts.	delinea.platform/analytics/alerts/update
Update Behavioral Analytics Notes	Update behavioral analytics notes.	delinea.platform/analytics/notes/update
Update Behavioral Analytics Settings	Update behavioral analytics settings.	delinea.platform/analytics/settings/update
View Behavioral Analytics	View the Behavioral Analytics page (Insights > Behavioral Analytics).	delinea.platform/analytics/read
View Behavioral Analytics Alerts	View behavioral analytics alerts.	delinea.platform/analytics/alerts/read
View Behavioral Analytics Events	View behavioral analytics events.	delinea.platform/analytics/events/read
View Behavioral Analytics Notes	View behavioral analytics notes.	delinea.platform/analytics/notes/read
View Behavioral Analytics Settings	View behavioral analytics settings.	delinea.platform/analytics/settings/read

Platform Audit Permissions

Permission Name	Description	Permission String
Add Session Recording Comments	Write comments in session recording. (Formerly Write Session Recording Comments.)	delinea.platform/audit/sessionrecording/comment/write
Modify Session Recording AIDA Settings	Access AIDA setting page.	delinea.platform/audit/sessionrecording/aida/settings
Read Audit events	Read all administrative and privileged activity events.	delinea.platform/audit/event/read
Read Own Audit events	Grants a user permission to read their own administrative and privileged activity events.	delinea.platform/audit/event/own/read
View AIDA results	Read AIDA results in session recording.	delinea.platform/audit/sessionrecording/aida/read

Roles and Permissions

Permission Name	Description	Permission String
View Authorized Session Recordings	Grants a user permission to view all authorized session recordings. (Formerly View All Session Recordings or View Session Recordings UI.)	delinea.platform/audit/sessionrecording/admin/read
View Own Session Recordings	Grants a user permission to open and view their personal session recordings.	delinea.platform/audit/sessionrecording/own/read
View Session Recording Comments	Read comments in session recording.	delinea.platform/audit/sessionrecording/comment/read

Delinea Expert Permissions

Permission Name	Description	Permission String
Access Delinea Expert	Chat with Delinea Expert.	delinea.platform/gpt/conversation/create
Configure Delinea Expert	Configure Delinea Expert.	delinea.platform/gpt/conversation/configure

Posture Check Permissions

Permission Name	Description	Permission String
Manage Checks	Manage posture checks.	delinea.platform/checks/manage
View Checks	View posture checks.	delinea.platform/checks/view

Identity Permissions

Permission Name	Description	Permission String
Administer RADIUS Server Configuration	Manage RADIUS client settings.	delinea.platform/identity/radius/administer
Manage Identity settings	Manage all Identity-related settings such as users, groups, policies, and more.	delinea.platform/identity/admin/manage
View Identity settings	View Identity-related settings such as users, groups, policies, and more.	delinea.platform/identity/admin/read
View RADIUS Server Configuration	View RADIUS client settings.	delinea.platform/identity/radius/read

Inventories Permissions

Permission Name	Description	Permission String
View Inventory	View inventories in the navigation menu.	delinea.platform/inventory/view

Analytics Management Permissions

Permission Name	Description	Permission String
Create Active Directory entities	Create Active directory entities.	delinea.platform/itp/activedirectory/create

Marketplace Permissions

Permission Name	Description	Permission String
Customize Marketplace Integration View	Customize Marketplace integration view.	delinea.platform/marketplace/integrationview/update
View Marketplace	Show Marketplace to the user.	delinea.platform/marketplace/read
View Marketplace Download Center	Show Marketplace Download Center to the user. (Formerly View Download Center.)	delinea.platform/marketplace/downloadcenter/read
View Subscriptions	View subscriptions in Marketplace.	delinea.platform/marketplace/subscriptions/read

Remote Access Permissions

Permission Name	Description	Permission String
Close PRA session	Close a Privileged Remote Access session.	delinea.platform/remoteaccess/sessions/end
Create Remote Applications	Create remote applications.	delinea.platform/remoteaccess/remoteapplication/create
Create Web Application	Create Web application.	delinea.platform/remoteaccess/webapplication/create
Delete Remote Applications	Delete remote applications.	delinea.platform/remoteaccess/remoteapplication/delete
Delete Web Application	Delete web application.	delinea.platform/remoteaccess/webapplication/delete
Download files with PRA	Download a file from the target system during a remote access session.	delinea.platform/remoteaccess/filetransfer/download
Launch PRA Session	Launch a Privileged Remote Access session.	delinea.platform/remoteaccess/session/launch
Launch Web Application	Launch web application.	delinea.platform/remoteaccess/webapplication/launch
Read Remote Applications	Read remote applications.	delinea.platform/remoteaccess/remoteapplication/read
Read Web Applications	Read web applications.	delinea.platform/remoteaccess/webapplication/read

Roles and Permissions

Permission Name	Description	Permission String
Update PRA Configuration	Update Privileged Remote Access Configuration.	delinea.platform/remotefaccess/configuration/update
Update Remote Applications	Update remote applications.	delinea.platform/remotefaccess/remotefapplication/update
Update Web Application	Update web application.	delinea.platform/remotefaccess/webapplication/update
Upload files with PRA	Upload a file to the target system during a remote access session.	delinea.platform/remotefaccess/filetransfer/upload
View PRA Configuration	View Privileged Remote Access Configuration.	delinea.platform/remotefaccess/configuration/read
View Secrets	View Secrets to launch Privileged Remote Access sessions.	delinea.platform/remotefaccess/secret/read

Vaultbroker Configuration Permissions

Permission Name	Description	Permission String
Allow creating vaultbroker connection information	Create the vaultbroker connection information. Still requires an admin to log into SecretServer first and configure the platform configuration.	delinea.platform/vaultbroker/vault/create
Allow editing vaultbroker connection information	Modify the vaultbroker connection information.	delinea.platform/vaultbroker/vault/update

Secret Server Permissions

Permission Name	Description	Permission String
Access Offline Secrets on Mobile	User can cache their secrets in the Secret Server mobile application for offline use. This permission does not automatically come with the Administrator role.	delinea.vault/secretserver/secret/mobile/offlinesecrets/allow
Add Custom Audit Entry for Secrets	Make a custom audit entry when accessing a secret using the web services API.	delinea.vault/secretserver/secret/customaudit/create
Add Secret	Create new secrets. The Add permission no longer includes the role permission <i>View Secret</i> .	delinea.vault/secretserver/secret/create

Roles and Permissions

Permission Name	Description	Permission String
Add Users or Groups From Identity	Search for users and groups from Identity sources and add those users or groups to Secret Server.	delinea.vault/secretserver/administration/identity/usersandgroups/add
Administer Analytics Challenge	Allows user to be challenged by analytics if their behavior deviates from their normal behavior and meets requirements specified by analytics. Administrators do not have this permission by default.	delinea.vault/secretserver/administration/securityanalytics/accesschallenge/allow
Administer Application Accounts in Secret Server	Create application user accounts to be used exclusively for accessing Secret Server via the API. Formerly Create Application Account.	delinea.vault/secretserver/administration/users/applicationaccounts/create
Administer Auto Export	Do everything the other automatic export permissions allow and edit the automatic export configuration.	delinea.vault/secretserver/administration/autoexport/administer
Administer Custom Columns on Secret Templates	Enable the Expose for Display setting of a secret's template field to make it available for use in Dashboard custom columns.	delinea.vault/secretserver/administration/secrettemplate/customcolumns/administer
Administer Custom Password Requirements	View and edit custom password requirements that can be configured under the Security tab for individual secrets.	delinea.vault/secretserver/administration/passwordrequirements/custom/administer
Administer Devops Secret Vault Tenants	Add, remove, and edit DSV tenants that automatically synchronize with Secret Server on a schedule.	delinea.vault/secretserver/administration/devopssecretvault/tenants/administer
Administer Disaster Recovery	Configure instances as data sources or replicas for disaster recovery; initiate or test data replication and view related logs and audits.	delinea.vault/secretserver/administration/disasterrecovery/administer

Roles and Permissions

Permission Name	Description	Permission String
Administer Distributed Engine Configuration	Update the Distributed Engine configuration.	delinea.vault/secretserver/administration/distributedengine/administer
Administer DoubleLock Keys	View, edit, create, and disable DoubleLock keys. A DoubleLock key acts as a separate encryption key to protect your most sensitive secrets. This option allows users to access and use the DoubleLocks link on the Administration page.	delinea.vault/secretserver/administration/doublelockkeys/administer
Administer Dual Control Settings	View, edit, create, and disable Dual Control settings for reports and recorded sessions.	delinea.vault/secretserver/administration/dualcontrol/administer
Administer Event Subscriptions	View, edit, and create event subscriptions.	delinea.vault/secretserver/administration/eventsubscriptions/administer
Administer Export	View the export log and export secrets to which they have access to a clear text, CSV file.	delinea.vault/secretserver/administration/export/administer
Administer HSM Configuration	Change configuration or disable the use of a Hardware Security Module (HSM).	delinea.vault/secretserver/administration/hsm/administer
Administer Jumpbox	Create, edit, or deactivate jump server routes.	delinea.vault/secretserver/administration/jumpboxroutes/administer
Administer Key Management	Enable, change, or disable the Key Management (Secret Server Cloud only).	delinea.vault/secretserver/administration/keymanagement/administer
Administer Platform Integration	Manage the Secret Server connection to the Delinea Platform.	delinea.vault/secretserver/administration/platformintegration/administer
Administer Platform Migration	Manage the Secret Server migration to the Delinea Platform.	delinea.platform/identity/radius/administer

Roles and Permissions

Permission Name	Description	Permission String
Administer Remote Password Changing Settings	Turn Heartbeat and Remote Password Changing on and off globally. Also allows users to create new password changers and install password changing agents on remote machines.	delinea.vault/secretserver/administration/remotepasswordchanging/administer
Administer SSH Cipher Suite	View and edit the SSH Cipher Suite.	delinea.vault/secretserver/administration/sshciphersuite/administer
Administer SSH Menus	Create and edit SSH Menus, used in allowlisting commands that can be used on a SSH session.	delinea.vault/secretserver/administration/sshmenus/administer
Administer Secret Encryption Key Rotation	Start a process that rotates the Secret encryption keys.	delinea.vault/secretserver/administration/encryptionkeys/rotate
Administer Secret Policy	Create and edit Secret Policies.	delinea.vault/secretserver/administration/secretpolicy/administer
Administer Secret Server Configuration	View and edit general configuration options. For example, a user with this role permission can turn on Force HTTPS/SSL and disable Allow Remember Me.	delinea.vault/secretserver/administration/configuration/administer
Administer Secret Server Data	Manage metadata fields and sections added to secrets and users in Secret Server.	delinea.vault/secretserver/administration/metadata/administer
Administer Secret Server Folders	View, edit, create, move, and delete folders. Users still need the relevant view, edit, and owner permissions on the folders to perform these tasks.	delinea.vault/secretserver/administration/folders/administer
Administer Secret Server Lists	Add, remove, and modify lists and list contents in Admin > Lists.	delinea.vault/secretserver/administration/lists/administer
Administer Secret Server Maintenance	Administer Secret Server maintenance.	delinea.vault/secretserver/administration/maintenancemode/administer

Roles and Permissions

Permission Name	Description	Permission String
Administer Secret Server Password Requirements	View and edit character sets and password requirements.	delinea.vault/secretserver/administration/passwordrequirements/administer
Administer Secret Server Pipelines	Create, edit, and remove event pipelines and event pipeline policies.	delinea.vault/secretserver/administration/pipelines/administer
Administer Secret Server Reports	View, edit, delete, and create reports. Also allows users to customize report categories.	delinea.vault/secretserver/administration/reports/administer
Administer Secret Server Scripts	View, edit, and add PowerShell, SQL, and SSH scripts on the Scripts Administration page.	delinea.vault/secretserver/administration/scripts/administer
Administer Secret Server Security Configuration	View and edit security configuration options in Secret Server. Currently, these include enabling FIPS compliance mode and protecting the encryption key. Formerly Administer Security Configuration.	delinea.vault/secretserver/administration/securityconfiguration/administer
Administer Secret Server SSH Proxy Configuration	View and edit SSH Proxy settings.	delinea.vault/secretserver/administration/proxyingconfiguration/administer
Administer Secret Server System Logs	View and clear the System Log, which shows general diagnostics information for Secret Server.	delinea.vault/secretserver/administration/systemlog/administer
Administer Secret Server Teams	Create, delete, and view all teams.	delinea.vault/secretserver/administration/teams/administer
Administer Secret Templates	View, edit, disable, and create secret templates.	delinea.vault/secretserver/administration/secrettemplate/administer
Administer Workflows	Manage workflows (advanced access management).	delinea.vault/secretserver/administration/workflows/administer

Roles and Permissions

Permission Name	Description	Permission String
Advanced Import	Import secrets from an XML file. Users with the this permission can import groups, folders, site connectors, sites, and secret templates, without having to create a secret. Users must have the Secret Server permissions needed for the objects listed in the XML.	delinea.vault/secretserver/administration/import/advancedimport/allow
Allow List Secret Access For Assigning Policy	Users with list access to a secret can assign policies. Users need the view permission if they do not have this one.	delinea.vault/secretserver/administration/secretpolicy/listsecretaccessforassigningpolicy/allow
Assign Secret Policy	Assign Secret Policies to folders and secrets.	delinea.vault/secretserver/secretpolicy/assign
Assign Secret Server Pipelines	Assign an event pipeline policy to secret policies, or folders.	delinea.vault/secretserver/administration/pipelines/assign
Audit Secret Server Session Recordings	Users with at least List Access permission on a secret can access the session recording of the secret. Administrators do not have this permission by default.	delinea.vault/secretserver/secret/sessionrecording/auditor
Browse Secret Server Reports	Access reports restricted by permissions. Permissions are configurable at the category and report levels and share a similar inheritance model to secrets and folders. You can define users or groups with view or edit permissions for each category or report.	delinea.vault/secretserver/administration/reports/browse
Bypass Direct API Authentication Restriction	Ignore the PreventDirectApiAuthentication advanced setting and log in through the API with a non-application account	delinea.vault/secretserver/user/directapiauthenticationrestriction/bypass
Bypass SAML Login	Log in with local account without using SAML (Secret Server specific).	delinea.vault/secretserver/user/samllogin/bypass

Roles and Permissions

Permission Name	Description	Permission String
Copy Secret	Copy secrets when the user also has Own Secret role permission.	delinea.vault/secretserver/secret/copy
Create External Vault Links	Link external vaults in Secret Server.	delinea.vault/secretserver/externalvault/create
Create Root Folders in Secret Server	Create new folders at the root level of the folder structure.	delinea.vault/secretserver/administration/folders/rootfolders/create
Deactivate Secret	Mark secrets as deactivated.	delinea.vault/secretserver/secret/deactivate
Deactivate a Secret within a Report	Run the Delete Secrets action from a report.	delinea.vault/secretserver/administration/reports/secretfromreport/deactivate
Download Auto Export	View all automatic export tabs and download exports from cloud storage (Secret Server Cloud only).	delinea.vault/secretserver/administration/autoexport/download
Edit Secret	Without this permission, a user cannot edit secrets, regardless of the secret permission.	delinea.vault/secretserver/secret/update
Enable Unlimited Administrator in Secret Server	Turn on Unlimited Admin Mode. When this mode is enabled, users with the Unlimited Administrator role permission can view and edit all secrets in the system, regardless of permissions. You can assign Enable Unlimited Administrator in Secret Server to one user and Unlimited Administrator to another user. This would require one user to turn on the mode, which enables another user to view and edit secrets.	delinea.vault/secretserver/administration/unlimitedadmin/administer
Erase Secret	Permanently erase a secret (as opposed to deactivate a secret, which is reversible).	delinea.vault/secretserver/secret/delete
Expire Secrets from Reports	Expire secrets listed in a report.	delinea.vault/secretserver/administration/reports/secretsfromreport/expire

Roles and Permissions

Permission Name	Description	Permission String
Launch Secret in Secret Server	Launch a secret. Previously, a user could launch a secret if their user role had the View Secret permission. As of Version 11.5, a user needs this permission to launch. A user will also need the Secret Launch Remote Access (Platform) permission to be able to launch.	delinea.vault/secretserver/secret/launch
Own Secret	Perform advanced tasks on secrets the user “owns,” such as configuring expiration schedules, configuring the web launcher, converting secret template, and copying secrets.	delinea.vault/secretserver/secret/own
Personal Folder in Secret Server	Have personal folder when the global personal folders configuration options is enabled.	delinea.vault/secretserver/user/personalfolder/allow
Run Auto Export	View all automatic export tabs and run the export manually by clicking the Run Export button.	delinea.vault/secretserver/administration/autoexport/run
Run Disaster Recovery Replication	Initiate or test data replication.	delinea.vault/secretserver/administration/disasterrecovery/datareplication/run
Run Secret Server Scripts	Separates privileges in script management. Holders of the View Scripts role permission cannot execute test runs of scripts, and this permission must be assigned to perform this task.	delinea.vault/secretserver/administration/scripts/run
Secret Force Check In	Force a secret that is checked out by another user to be checked in.	delinea.vault/secretserver/secret/checkin/override

Roles and Permissions

Permission Name	Description	Permission String
Secret Server Web Services Impersonate	Send an approval request to act as another user within their organization when accessing Secret Server programmatically. Administrators do not have this permission by default.	delinea.vault/secretserver/user/impersonatewebservices/allow
Unlimited Administrator in Secret Server	View and edit all secrets in the system, regardless of permissions, when Unlimited Admin Mode is on. Another user with the Enable Unlimited Administrator in Secret Server role permission still needs to turn this mode on.	delinea.vault/secretserver/administration/unlimitedadmin/unlimitedadministrator
Unrestricted by Teams in Secret Server	View all users, groups, and sites, regardless of team affiliation. Essentially, teams do not exist for the users with this permission, and the Teams page is not available to them. The default user role has this permission.	delinea.vault/secretserver/user/unrestrictedbyteams/allow
User Audit Expire Secrets	View the User Audit report, which shows all secrets accessed by a particular user in a specified date range. Also allows the user to force expiration on all these secrets, which would make Secret Server automatically change the password.	delinea.vault/secretserver/administration/useraudit/expiresecrets
View Advanced Secret Options	View the Remote Password Changing, Security, and Dependency tabs on a Secret they have access to.	delinea.vault/secretserver/secret/advancedoptions/read
View Auto Export	View all automatic export tabs.	delinea.vault/secretserver/administration/autoexport/read
View Devops Secret Vault Tenants	View (not edit) the DSV tenants set to synchronize with Secret Server.	delinea.vault/secretserver/administration/devopssecretvault/tenants/read
View Disaster Recovery	View configuration, logs and audits for Disaster Recovery.	delinea.vault/secretserver/administration/disasterrecovery/read

Roles and Permissions

Permission Name	Description	Permission String
View Distributed Engine Configuration	View the Distributed Engine configuration.	delinea.vault/secretserver/administration/distributedengine/read
View DoubleLock Keys	View which DoubleLock keys exist in the system.	delinea.vault/secretserver/administration/doublelockkeys/read
View Dual Control Settings	View configured Dual Control settings for reports and secret sessions.	delinea.vault/secretserver/administration/dualcontrol/read
View Enterprise Objects	View user and secret metadata.	delinea.vault/secretserver/administration/enterpriseobjects/read
View Event Subscriptions	View event subscriptions.	delinea.vault/secretserver/administration/eventsubscriptions/read
View Export	View the export log of the system to see when users exported secrets. Does not allow a user to export.	delinea.vault/secretserver/administration/export/read
View External Vaults	View external vaults in Secret Server.	delinea.vault/secretserver/externalvault/read
View HSM Configuration	View the Hardware Security Module (HSM) configuration settings.	delinea.vault/secretserver/administration/hsm/read
View Inactive Secrets	View secrets that have been deleted in the system.	delinea.vault/secretserver/secret/inactivesecrets/read
View Jumpbox	View the details of all jump server routes in the Admin Jumpbox Route page but not make any changes.	delinea.vault/secretserver/administration/jumpboxroutes/read
View Key Management	View the Key Management settings (Secret Server Cloud only).	delinea.vault/secretserver/administration/keymanagement/read

Roles and Permissions

Permission Name	Description	Permission String
View Launcher Password on Secrets	Unmask the password on the view screen of secrets with a launcher. Typically, this includes Web Passwords, Active Directory accounts, Local Windows accounts, and Linux accounts.	delinea.vault/secretserver/secret/launcherpassword/read
View Platform Integration	View the Secret Server connection to the Delinea Platform.	delinea.vault/secretserver/administration/platformintegration/read
View Remote Password Changing Settings	View, but not edit, heartbeat and remote password changing settings.	delinea.vault/secretserver/administration/remotepasswordchanging/read
View SSH Cipher Suite	View (only) the SSH Cipher Suite.	delinea.vault/secretserver/administration/sshciphersuite/read
View SSH Menus	View existing SSH menus, used in allow-listing commands that can be used on a SSH session.	delinea.vault/secretserver/administration/sshmenus/read
View Secret	View secret. Without this permission, a user cannot view secrets, regardless of the secret permission.	delinea.vault/secretserver/secret/read
View Secret Audit	View Secret Audit.	delinea.vault/secretserver/secret/audit/read
View Secret Password and Private Key History	View the history of passwords, private keys, or passphrases in both old and new UI.	delinea.vault/secretserver/secret/passwordandprivatekeyhistory/read
View Secret Policy	View, but not edit, secret policies.	delinea.vault/secretserver/administration/secretpolicy/read
View Secret Server Advanced Dashboard	View advanced dashboard. Without this permission, users can only view the basic dashboard.	delinea.vault/secretserver/user/advanceddashboard/read
View Secret Server Configuration	View, but not edit, general configuration settings.	delinea.vault/secretserver/administration/configuration/read

Roles and Permissions

Permission Name	Description	Permission String
View Secret Server Folders	View, but not edit, folders in the system.	delinea.vault/secretserver/administration/folders/read
View Secret Server Lists	View lists and list contents in Admin > Lists.	delinea.vault/secretserver/administration/lists/read
View Secret Server Password Requirements	View character sets and password requirements.	delinea.vault/secretserver/administration/passwordrequirements/read
View Secret Server Pipelines	View event pipeline policies and policy activities.	Delinea.vault/secretserver/administration/pipelines/read
View Secret Server Reports	View, but not edit, reports.	delinea.vault/secretserver/administration/reports/read
View Secret Server Scripts	View PowerShell, SQL, and SSH scripts on the Scripts Administration page.	delinea.vault/secretserver/administration/scripts/read
View Secret Server Security Configuration	View the security configuration of Secret Server. Formerly View Security Configuration.	delinea.vault/secretserver/administration/securityconfiguration/read
View Secret Server Security Hardening Report	View the Security Hardening Report.	delinea.vault/secretserver/administration/securityhardeningreport/read
View Secret Server Session Recording Audit	See who has viewed a session recording in the secret audit.	delinea.vault/secretserver/administration/sessionrecording/audit/read
View Secret Server SSH Proxy Configuration	View, but not edit, SSH Proxy settings.	delinea.vault/secretserver/administration/proxyingconfiguration/read
View Secret Server System Logs	View (only) the System Log, which shows general diagnostics information for Secret Server.	delinea.vault/secretserver/administration/systemlog/read
View Secret Server Teams	View all teams. This is essentially a read-only Administer Teams.	delinea.vault/secretserver/administration/teams/read

Permission Name	Description	Permission String
View Secret Server Templates	View, but not edit, Secret Templates.	delinea.vault/secretserver/administration/secrettemplate/read
View Secret Session Recording	View recorded sessions within Secret Server.	delinea.vault/secretserver/administration/sessionrecording/read
View Unlimited Administrator Audit	View the Unlimited Admin Mode configuration and the Unlimited Admin Mode audit log. Formerly View Unlimited Admin Configuration.	delinea.vault/secretserver/administration/unlimitedadmin/read
View User Audit Report	View, but not edit, the User Audit Report.	delinea.vault/secretserver/administration/useraudit/report/read
View Workflows	View, but not edit, workflows used for multi-tier secret-access approvals and secret erase requests.	delinea.vault/secretserver/administration/workflows/read

Platform Engine Management

The Delinea Platform manages and protects endpoints using small software packages called Delinea Platform Engines that handle the orchestration of Delinea services called **workloads**.


The platform's Engine Management feature provides administrators with a single interface for managing these engines and workloads, which are automatically updated and maintained after installation – removing the need for separate installers and management processes traditionally necessary on individual machines.

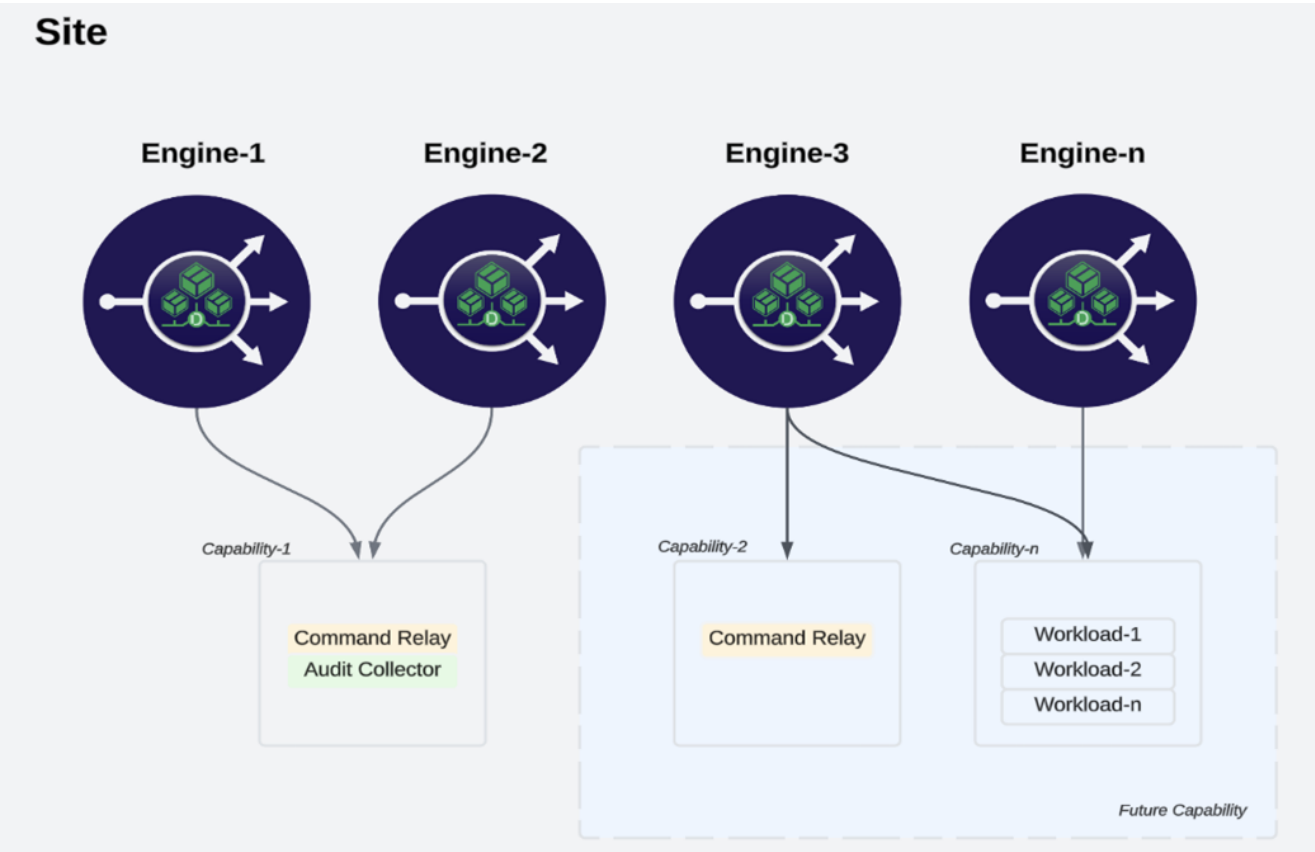
Engine Management Components

The components of the Engine Management feature are as follows:

Component	Description
Site	A group of engines selected on a common principle, such as network or subnet, geographical location (office, city, continent), data center, or any other characteristics. Workload settings are organized at the site level.

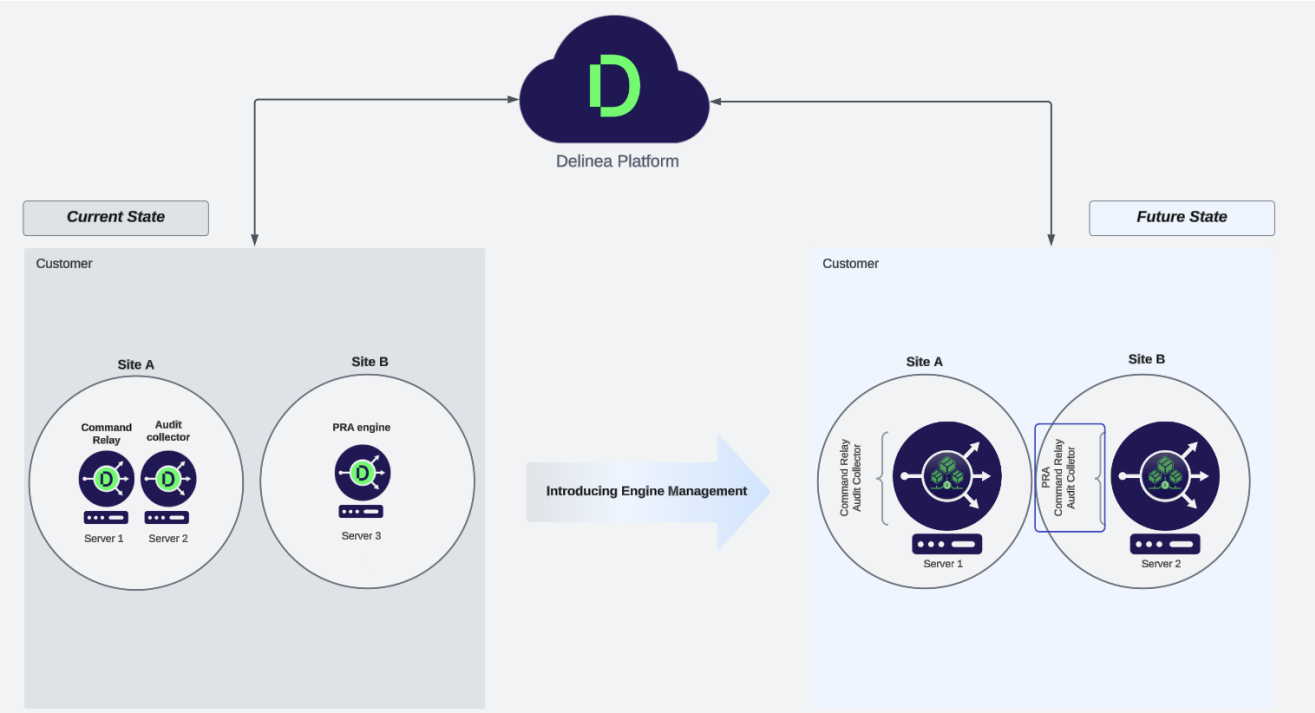
Component	Description
Engine	A system daemon that runs on an endpoint and exchanges data with the Delinea Platform. It sends information about the engine's application and capabilities, and it receives information about the applications and workloads it needs to execute. It executes the workloads and reports status to the platform.
Workload	Workloads are applications that are managed by Platform Engines. They perform functions like facilitating communications between the platform and downstream assets, capability-specific computations like small-scale or large-scale analytics, pre-processing and collation of data, and so on.
Capabilities	A set of predefined workloads that users can run on an engine. Users can choose one or more capabilities for each engine, based on their specific business use case.

 **Note:** The Delinea Platform Engine and its workloads run on a server endpoint, but they exchange data with the Delinea Platform.



Engine Management Architecture


The following diagram illustrates customer options for running one workload per engine or running multiple workloads on a single engine.



Server Hardware and System Requirements

The following table provides details about the hardware and other system requirements for the server where the Platform Engine is installed, as well as the related workloads for Audit Collector, Command Relay, and Privileged Access Management.

Requirements	Details
Supported Windows Operating Systems	<ul style="list-style-type: none">Windows 10, 11Windows Server 2022, 2019

Requirements	Details
Supported Linux Operating Systems	<ul style="list-style-type: none"> Amazon Linux 2 Amazon Linux 2023 Debian 11, 12 Red Hat Enterprise Linux 8, 9 Ubuntu Linux 20.04, 22.04, 23.10, 24.04
CPU	x86-64 based processors at 2.5 GHz or higher, with two or more cores, are recommended for production use.
Memory	<ul style="list-style-type: none"> For non-production: 2 GB For production: 8 GB
Storage	<p>500 MB or more recommended for installation and run-time needs.</p> <p> Note: Logging retention may increase the storage requirements.</p>
Ports	Port 443 (outbound only) must be open for the Platform Engine to send encrypted information to the platform through the CloudAMQP messaging service. See " Network Communication " on page 239.

Queue - Fully Qualified Domain Names (CloudAMQP)

The following Fully Qualified Domain Names are deployed by CloudAMQP using public IP ranges of Amazon, Azure, DigitalOcean, and Google Cloud, and are used by the Platform Engine to facilitate communication with the platform by means of encrypted messages over the CloudAMQP messaging service.

Outbound firewall rules should include the following Fully Qualified Domain Names (selected by databoundary), rather than static IP ranges of these URLs, as these IP ranges can change.

Australia	technical-blond-elk.rmq2.cloudamqp.com
Canada	smart-orange-gibbon.rmq2.cloudamqp.com
EU	young-azure-hare.rmq2.cloudamqp.com
SEA	hippy-fuchsia-woodpecker.rmq2.cloudamqp.com
UAE	young-olden-buffalo.rmq6.cloudamqp.com
UK	giant-maroon-bullfrog.rmq3.cloudamqp.com

US	dramatic-coral-crow.rmq2.cloudamqp.com loud-beige-duckbill.rmq5.cloudamqp.com fast-green-crab.rmq2.cloudamqp.com bobbish-coral-anteater.rmq4.cloudamqp.com anteater.rmq4.cloudamqp.com
----	--

**Notes:**

- Platform Engines cannot be installed on domain controllers.
- When using PowerShell, version 7.3 is recommended for optimal performance, while version 5.1 may result in suboptimal performance.
- Platform Engines use the CloudAMQP service to queue encrypted messages which are then consumed by Engine Management, and vice-versa. These queues are separated by regional databoundary and messages are encrypted/decrypted by tenant. In order to have successful communication between Engine and Engine Management, the outbound message queue URLs must be allowed at the Engine endpoint, along with an open port 443 (TLS MQTT over websockets). See the next section, *Network Communication*.

Engine Security

Platform Engines retrieve workloads from the Delinea Platform, which supplies securely signed packages for the engine to download.

The Platform Engine only runs workload deployment binaries that are both signed and trusted.

During deployment execution, Platform Engines maintain a file integrity check for both the working and binary directories. Any unauthorized modifications to these directories will render the deployment invalid and trigger its recycling, which may require downloading the deployment packages again.

Platform Engines send heartbeats to the platform to fetch configuration updates using a stamp. This stamp verifies whether the engine configuration matches the machine's configuration. These heartbeats are dispatched every five minutes, ensuring prompt detection of any new updates during this interval.

Engine Status

Status	Description
Pending	The engine has been installed on a supported OS but has not been approved, or it is in the process of self-update. This includes the time an engine spends waiting to be approved as well as the time spent downloading packages over the network.
Online	The engine has been approved, and workloads have been created. At least one deployment is still running, or it is in the process of starting or restarting.

Status	Description
Offline	The engine status could not be obtained. This status typically occurs due to an error in communicating with the engine or the machine where this engine should be running.
Failed	All deployments of the engine have been terminated, and at least one deployment has been terminated in failure. That is, the deployment either exited with a non-zero status or was terminated by the system.

Account Permissions and Roles

The table below describes each permission available with an Engine Management domain admin account.

Permissions	Description	Permission List	User	Admin
Add Engine	Ability to create a new engine.	delinea.enginepool/engine/create	N/A	Yes
Delete Engine	Ability to delete an engine.	delinea.enginepool/engine/delete	N/A	Yes
Update Engine	Ability to edit an engine.	delinea.enginepool/engine/update	N/A	Yes
Create a Site	Ability to create a new site.	delinea.enginepool/site/create	N/A	Yes
Delete a Site	Ability to delete a site.	delinea.enginepool/site/delete	N/A	Yes
Update a site	Ability to update a site.	delinea.enginepool/site/update	N/A	Yes
List Engines	Ability to view summary information about all engines.	delinea.enginepool/engine/list	Yes	Yes

Permissions	Description	Permission List	User	Admin
List Sites	Ability to see and choose sites through the platform UI, such as in a dropdown list of sites in the PRA setup page. This permission does not grant the ability to view and modify sites through the Engine Management page. For that, the Manage Sites permission is required.	delinea.enginepool/site/list	Yes	Yes
Manage Sites	Ability to view summary information about all sites and make changes.	delinea.enginepool/site/manage	N/A	Yes
View Engine	Ability to read full information about an engine.	delinea.enginepool/engine/read	Yes	Yes
View Site	Ability to read full information about a site.	delinea.enginepool/site/read	Yes	Yes
Retrieve Workload Definition	View (not edit) workflows used for multi-tier secret-access approvals and secret erase requests.	delinea.registration/workloaddefinition/read	No	Yes

Network Communication

Upstream and Downstream

The Engine Management service can manage Platform Engines on millions of endpoints per tenant. To achieve high availability, the request from the engine to the server is sent only once during the engine registration. The rest of the time, communication is carried over message queues.

Upstream communication includes every message from the engine to the server. Downstream communication is from the server to the engines. Downstream doesn't have a gRPC option.

- The Platform Engine can get a new configuration from the server passively. This means that engines that aren't active (no current workloads) can get the up-to-date configuration from the server. This reduces the load on the system.
- Platform Engines always send their heartbeats upstream to the server.
- If the server determines the engine is out of sync, it sends a single message to the groups the engine belongs to. The engine that forced that message, and all others that have the wrong group stamp, will update. This strategy reduces the load on the bus, and engines eventually coalesce. If an engine stamp itself is outdated, the server sends a message on the engine topic for the engine to update.
- The ultimate goal is to minimize the engine-server communication: outbound messages upstream from the engine to the server and inbound messages downstream from the server to the engine.

Types of messages sent:

- Engine registration (upstream, gRPC)
- Workload registration (upstream, gRPC)
- Engine heartbeats (upstream, engine to server)
- Group changes (downstream, server to applicable engines)
- Workload changes (downstream, server to applicable engines)
- Engine changes (downstream, server to specific engine)
- Engine upgrade (downstream, server to applicable engines)
- Engine uninstall (downstream, server to specific engine)

Protocols

gRPC (upstream). The gRPC protocol is used for the engine registration. After registration:

- The server sends its new configuration downstream to the engine.
- The IT Admin can request a new configuration using the gRPC call.

MQTT (upstream / downstream). Message Queuing Telemetry Transport is an OASIS standard messaging protocol for the Internet of Things (IoT). MQTT is the preferred protocol for sending upstream and downstream fire-and-forget messages. MQTT is used when the message to be sent is under the maximum payload length of 64KB. MQTT uses TLS port 443.

AMQP (upstream / downstream). Advanced Message Queuing Protocol is an open standard for passing business messages between applications or organizations. When the message payload exceeds 64KB, AMQP protocol is used as the message transfer protocol. AMQP uses TLS port 5672.

HTTP Proxy Setup

Delinea Platform Engine supports communication through an HTTP proxy.

Engines automatically adopt the system-wide configuration of a proxy from the operating system's settings or from the following environment variables:

- HTTP_PROXY: The proxy server used on HTTP requests.
- HTTPS_PROXY: The proxy server used on HTTPS requests.
- ALL_PROXY: The proxy server used on HTTP and HTTPS requests when HTTP_PROXY or HTTPS_PROXY are not defined.
- NO_PROXY: A comma-separated list of hostnames that should be excluded from proxying. Asterisks are not supported for wildcards; use a leading dot if you want to match a subdomain.

Examples:

NO_PROXY=.example.com (with leading dot) matches www.example.com, but does not match example.com.

NO_PROXY=example.com (without leading dot) does not match www.example.com.

To override the system-wide proxy settings for the engine, define these environment variables for the engine's service process. This process runs as the account LocalSystem, and this account does not inherit the Windows system proxy settings. You must specify the proxy settings for the engine directly. There are two techniques you can use:

- "Specifying HTTP Proxy Settings Using bitsadmin" below
- "Specifying HTTP Proxy Settings Using the Registry" on the next page

Specifying HTTP Proxy Settings Using bitsadmin

For this procedure, you will need to know the IP address or DNS of the proxy server and the port.

For more information about the utility you'll use in these steps, see [bitsadmin util and setieproxy](#) in the Microsoft documentation.

1. At the command line on each server endpoint where the Delinea Platform Engine is installed, run the following command:

```
C:\windows\System32\bitsadmin.exe /util /SetIEProxy LocalSystem Manual_proxy  
http://<proxy-ip>:<proxy-port> ""
```

- Substitute your own IP address and port for <proxy-ip>:<proxy-port>.
- Between the quote marks (""), specify a space-delimited list of host names or IP addresses for which you do not want transfers to be routed through a proxy. If you do not want to specify this bypass list, leave the quotes empty or use the keyword NULL.

2. Restart the engine service.

- a. Open the Services list, either through the Search bar or by running `services.msc` in a command terminal window.
- b. In the Services window, right-click the **Delinea Engine-<version>** service and select **Restart**.



Note: If the engine is updated to a different version number later, you must specify the proxy settings again for Delinea.Engine-<new-version>.

Specifying HTTP Proxy Settings Using the Registry

If you prefer to use the Windows registry, or if the `bitsadmin` technique did not work in your situation, use the procedure in this section.

On each server endpoint where the Delinea Platform Engine is installed:

1. Open the Windows Registry Editor, either through the Search bar or by running `regedit.exe` in a command terminal window.

2. Open the following registry key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Delinea.Engine-<version>`

For example:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Delinea.Engine-1.9.185`

3. Within this key, add a value of type `REG_MULTI_SZ` and name it `Environment`.

For more information, see [Registry value types](#) in the Microsoft documentation.

4. Set the new `Environment` value to the following:

```
HTTP_PROXY=http://<proxy-ip>:<proxy-port>
HTTPS_PROXY=http://<proxy-ip>:<proxy-port>
NO_PROXY=localhost,127.0.0.*
```

5. Restart the engine service.

- a. Open the Services list, either through the Search bar or by running `services.msc` in a command terminal window.
- b. In the Services window, right-click the **Delinea Engine-<version>** service and select **Restart**.



Note: If the engine is updated to a different version number later, you must specify the proxy settings again for `Delinea.Engine-<new-version>`.

About Delinea Platform Engine Sites

A site functions as a logical divider for engines, closely resembling network demarcations.

A site doesn't restrict the workloads an engine can run, but it does influence the engine's communication scope. For instance, a site could correspond to a data center or a main office.

- **Similar term:** Zone
- **Definition:** A logical grouping of engines based on location, most likely a network boundary.
- **Examples:**
 - Data center 1
 - Remote Office
 - DMZ

About the Delinea Platform Engine

The Platform Engine functions as a system daemon on an endpoint (server or workstation), to facilitate data exchange with the Delinea Platform. The Platform Engine transmits data to the platform about the endpoint where it is installed, and it receives instructions from the platform about the workloads it should execute.

- **Similar terms:** Node
- **Function:** When installed within an environment (on either a physical or virtual machine), the Windows service/Linux daemon enables the execution of authorized and validated packages from the platform's various services.
- **Installation Process:** Click **Add Engine** from your chosen engine site, and an installation script is displayed. To install the engine, copy and run this script as an administrator. After installation, the engine is registered with the Engine Management service.
- **Data Transmitted:**
 - The engine assumes the responsibilities of downloading, executing, and monitoring package processes.
 - Communication between the engine and the Engine Management service includes registration, authentication, receipt of communication configuration, and relevant manifests.
- **Organization:**
 - Engines are grouped into sites.
 - An engine can only be assigned to a single site.
 - An engine cannot be moved to a new site.

Managing Engine Sites

This section tells how to get a quick preview, create, edit, and delete engine sites.

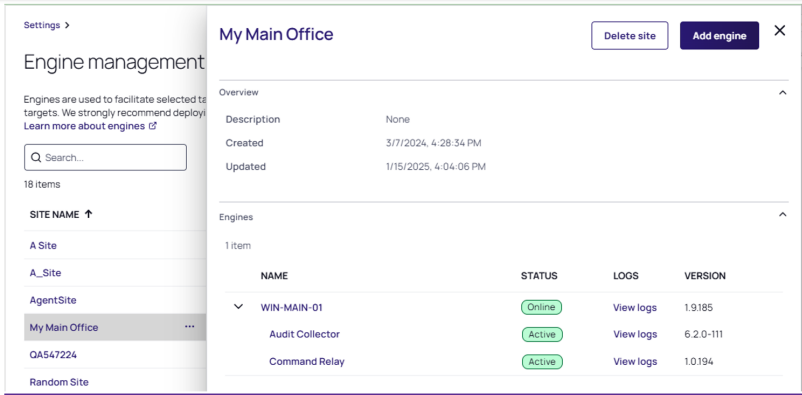
Engine Site Preview Panel

The Site preview panel gives an overall look at the health of the engines and workloads. It provides access to view the logs so you can quickly evaluate and locate information to help troubleshoot any issues.

To display the preview panel:

1. In the left navigation, click **Settings**, then **Engine Management**.
2. Find your site in the list, and click in any blank area of that row; for example, the white space between the site name and its description.

Platform Engine Management

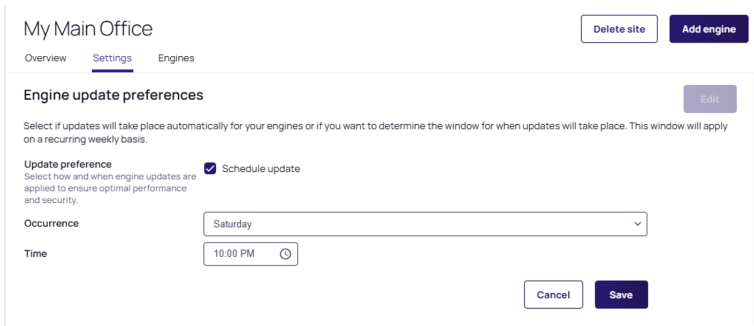


Creating a Site

1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Click **Create Site**.
3. Enter a **Site name** and **Description**.
4. Click **Save**.

Editing a Site

1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Click the name of the site. The site page opens to the Overview tab.
3. Click **Edit** to update the **Site name** or **Description**.
4. Select the **Settings** tab.
5. (Optional) You can schedule weekly updates for the engines, instead of accepting the default automatic updates.
 - a. In **Engine update preferences**, click **Edit**.
 - b. Select **Schedule update**.
 - c. In **Occurrence**, choose the day of the week, and in **Time**, set the time of day.
 - d. Click **Save**.



6. Edit the settings for your workloads. These workload settings must be specified before installing an engine. For example, in **Audit Collector**, click **Edit**, then fill in the required values. See "Editing Audit Collector Settings" on page 257.
7. In **Command Relay**, click **Edit**, then fill in the required values. These workload settings must be specified before installing an engine. See "Editing Command Relay Settings" on page 260.

The screenshot shows the 'My Main Office' settings page. At the top, there are tabs for 'Overview', 'Settings', and 'Engines'. Below the tabs, there are two main sections: 'Engine update preferences' and 'Command Relay'. The 'Engine update preferences' section has an 'Edit' button. The 'Command Relay' section has an 'Edit' button. At the bottom, there are 'Cancel' and 'Save' buttons.

Deleting a Site

1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Select a site.
3. Click **Delete Site**.

The screenshot shows the 'My Main Office' settings page. At the top, there are tabs for 'Overview', 'Settings', and 'Engines'. Below the tabs, there is a 'Delete Site' button. Below the button, there is a table with the following data:

Site name	My Main Office
Description	HQ office

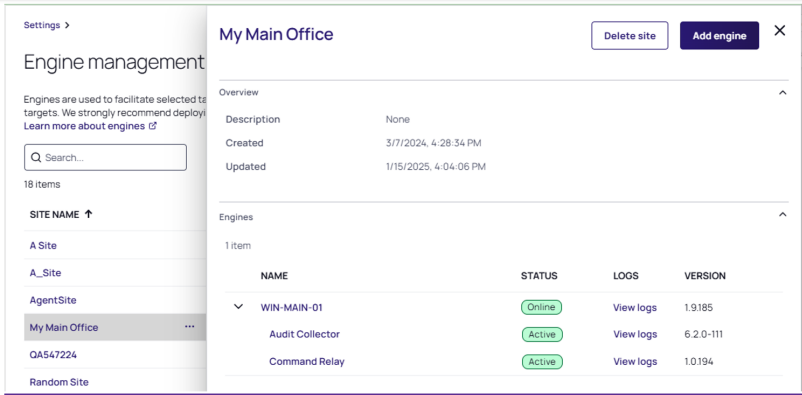


Notes:

- You cannot delete a site that still contains Platform Engines. First, remove all engines, then delete the site.
- You can perform the same action using quick actions in the site table or using the preview panel.

The following image shows the Delete button in the Site Preview panel.

Platform Engine Management

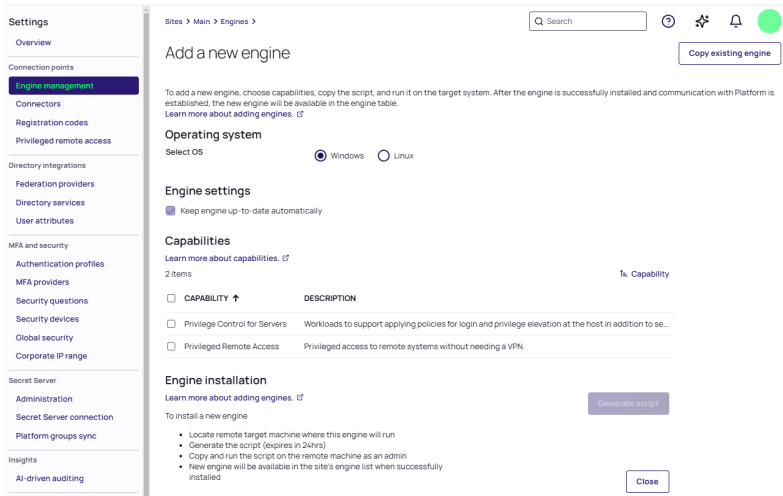


Managing Platform Engines

This section tells how to add, copy, add capabilities to, update, or uninstall a Platform Engine.

Adding a Platform Engine

1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Click the name of a site where you want to add an engine.
3. Click the **Engines** tab.
4. Click **Add Engine**. The **Add a new engine** page is displayed.



5. Select the OS (**Windows** or **Linux**).
6. Select the desired **Capabilities**.
7. Click **Generate script**. A device code is generated for the new engine installation script. This device code expires in 24 hours. If the engine is not installed by then, you must regenerate the script.
8. Once the script is generated, click **Copy script to clipboard**.

9. Access the target system.
10. Run the script from your clipboard on the target system with elevated privileges.

The installation script for Windows automates the process of downloading and installing the engine.

```

Downloading packages. This may take a moment...
[11:44:42 INF]
[11:44:43 INF]
[11:44:43 INF] Platform Engine
[11:44:43 INF]
[11:44:43 INF]
[11:44:43 INF]
[11:44:43 INF]
[11:44:43 INF]
[11:44:43 INF]
[11:44:43 INF] ConfigureAsync
[11:44:43 INF] Version: 1.9.124
[11:44:43 INF] Is configured: false
[11:44:43 INF] Copying the Shell to the destination folder
[11:44:43 INF] Copying the Precheck executable to the destination folder
[11:44:43 INF] Copying scripts to the destination folder
[11:44:43 INF] Creating data folder
[11:44:43 INF] Configuring to run the Shell as service
[11:44:43 INF] RegisterService
[11:44:43 INF] LogonAccount after transforming: NT AUTHORITY\SYSTEM, user: SYSTEM, domain: NT AUTHORITY
[11:44:43 INF] Verifying if the account has LogonAsService permission
[11:44:43 INF] Account SYSTEM has 'SeServiceLogonRight' right.
[11:44:43 INF] Account: NT AUTHORITY\SYSTEM already has Logon As Service Privilege.
[11:44:43 INF] Create local group and grant folder permission to service logon account.
[11:44:44 INF] Registering highest available version 1.9.124.
[11:44:44 INF] Calculated unique group name ShellService_G8fab8
[11:44:44 INF] Trying to create group ShellService_G8fab8
[11:44:44 INF] Local Group 'ShellService_G8fab8' created
[11:44:44 INF] Trying to add userName NT AUTHORITY\SYSTEM to the group ShellService_G8fab8
[11:44:44 INF] Account 'NT AUTHORITY\SYSTEM' is added to local group 'ShellService_G8fab8'.
[11:44:44 INF] Set full access control to group for the folder C:\ProgramData\Delinea Engine\1.9.124
[11:44:44 INF] Trying to open SCManager.
[11:44:44 INF] Opened SCManager. Trying to create service Delinea.Engine-1.9.124
[11:44:44 INF] ServiceInstalled Delinea.Engine-1.9.124
[11:44:44 INF] ServiceDescriptionSet Delinea.Engine-1.9.124
[11:44:44 INF] ServiceRecoveryOptionSet Delinea.Engine-1.9.124
[11:44:44 INF] ServiceDelayedStartOptionSet Delinea.Engine-1.9.124
[11:44:44 INF] ServiceConfigured Delinea.Engine-1.9.124
[11:44:45 INF] Configuration was successful
[11:44:51 INF] Trying to start service
[11:44:55 INF] ServiceStartedSuccessfully Delinea.Engine-1.9.124
PS C:\Users\vboxuser\AppData\Local\Temp\3e7eb7ca-ff7b-49b4-8123-365e57076d35>

```

The installation script for Linux automates the process of downloading and installing the engine.

```
vboxadmin@ub0:~$ sudo ./Delinea.Engine-installer-XXXXXX; trap "sudo rm -rf $InstallDir" 0 1 2 3 15; cd $InstallDir; echo "Downloading packages. This may take a moment..."; URL='https://enginepool-downloads-dev.azureedge.net/shell-installer/latest/linux-x64.tgz'; curl -fLO $URL; gunzip -c *.tgz | tar -xf -; sudo ./Delinea.EnginePool.Engine.Installer.configure --device-code "eyJJJZCI6IjAxZGM3OGM0LTM0N2ItNGI4NS1mZQZLTmWnZQxMDhmM2U0MyIsIlRlbnFudFVybCICImh0dHBzOi8vcmlvdG9yYbS5ZWN1cmVwbGF0Zm9ybS5pbY8iLCJUZWSHbnRJZCI6Ijc2NWQzOWY0LWE1YTmtGNiZiO5ODkzLWUwZWmI4M2MOMTK4NiIsIkV4cGlyZXNBdCI6MTczMjA0NDgONX0=" --config-url "https://enginepoolupdatedev.blob.core.windows.net/engine-c\nonfiguration/2b1f5ea1-2b47-4868-a3fa-a951cbad2581");)
Downloading packages. This may take a moment...
% Total    % Received % Xferd   Average Speed      Time     Time       Time    Current
           Dload  Upload   Total       Spent      Left     Speed
100 133M  100 133M    0     0 1321k      0  0:01:43  0:01:43  --:--:-- 1593k
[21:36:08 INF]
[21:36:08 INF]
[21:36:08 INF] PlatformEngine
[21:36:08 INF]
[21:36:08 INF]
[21:36:08 INF]
[21:36:08 INF]
[21:36:08 INF]
[21:36:08 INF]
[21:36:08 INF]
[21:36:08 INF] ConfigureAsync
[21:36:08 INF] Version: 1.9.124
[21:36:08 INF] Is configured: False
[21:36:08 INF] Copying the Shell to the destination folder
[21:36:09 INF] Copying the Precheck executable to the destination folder
[21:36:09 INF] Copying scripts to the destination folder
[21:36:09 INF] Creating data folder
[21:36:09 INF] Configuring to run the Shell as service
[21:36:09 INF] RegisterService
[21:36:09 INF] Registering highest available version 1.9.124.
[21:36:09 INF] Writing systemd service file /etc/systemd/system/delinea-engine.service
[21:36:09 INF] Enabling systemd service...
[21:36:10 INF] Systemd service delinea-engine installed successfully
[21:36:10 INF] Configuration was successful
[21:36:11 INF] Trying to start the service...
[21:36:12 INF] Successfully started the service
vboxadmin@ub0:~$
```

After the engine is successfully installed and has established communication with the platform, the new engine appears in the engines table of your site on the platform.

Copying a Platform Engine

An engine's capabilities can be copied from an existing engine.

1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Click the name of a site where you want to add an engine.
3. Click the **Engines** tab.
4. Click **Add engine**.
5. Click **Copy existing engine**. The following dialog is displayed: **Choose an existing Windows engine to copy**.

Platform Engine Management

Choose an existing Windows engine to copy

Each engine contains associated capabilities. Hover over the count to view the capability types.

+

7 items Engine

ENGINE ↑	CAPABILITY	SITE	OS
☆ WIN-2019-LP	1	sometest	Windows
☆ TEST-01-1234	1	anotherstest	Windows
☆ ENGINE01	1	test	Windows
☆ ENGINE-02	2	NewSite	Windows
☆ QA-WIN2019	1	MySite	Windows
☆ WIN-1234-TEST	1	test	Windows
☆ WIN-VM-01	1	Site Lab	Windows

Cancel

6. Select the engine you wish to copy. The capabilities of the engine are automatically selected.
7. Click **Generate script**.
8. Once the script is generated, click **Copy script to clipboard**.

Adding Capabilities to a Platform Engine

You can add PCS and PRA capabilities to the Platform Engine using the workloads below.

- **Privilege Control for Servers:**
 - [Audit Collector Workload](#) (Windows)
 - [Command Relay Workload](#) (Windows)
- **Privileged Remote Access:**
 - [Privileged Remote Access Workload](#) (Windows and Linux)
- **ITP for Active Directory**
 - [ITP for Active Directory Workload](#) (Windows)

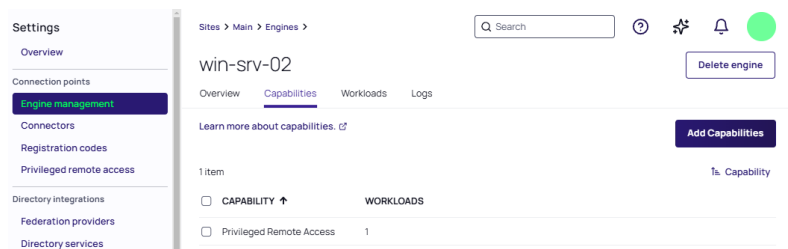
For details, see the following:

- [Engine Workloads](#)
- [Privilege Control for Servers](#)
- [Privileged Remote Access](#)

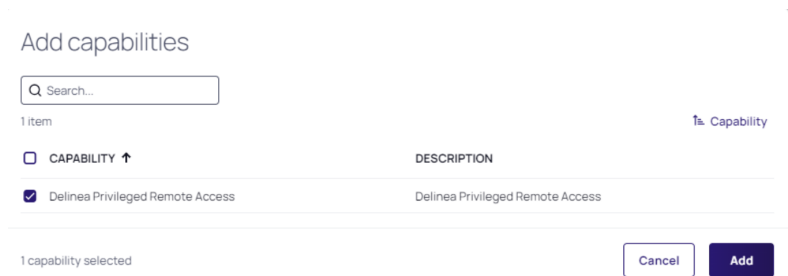
To add capabilities to an existing engine, follow the steps below.

Platform Engine Management

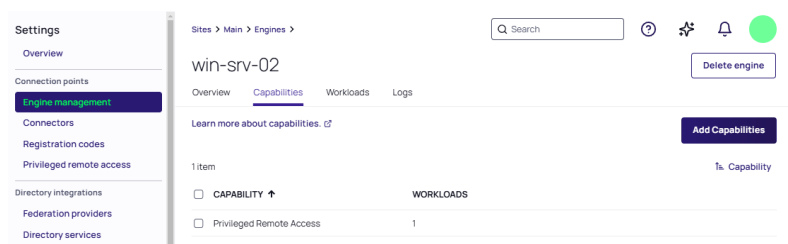
1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Click the name of a site where you want to add an engine.
3. Click the **Engines** tab.
4. Select the engine you wish to add capabilities to.
5. Click the **Capabilities** tab.



6. Click **Add Capabilities**. The Add capabilities dialog appears.



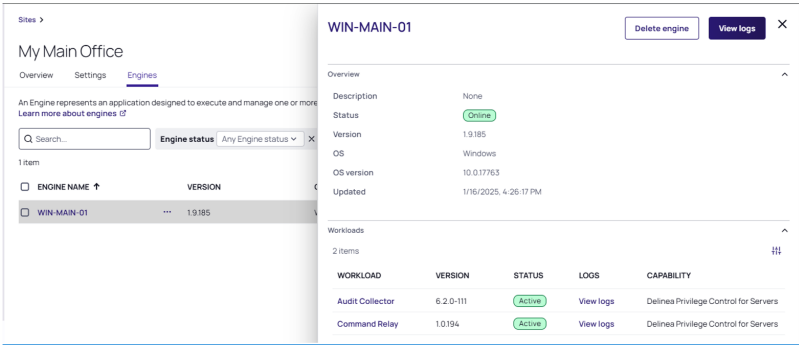
7. Select the capability you wish to add to the engine.
8. Click **Add**. The new capability is displayed in the capability table.



Automatic Platform Engine Update

The engines consistently transmit their status to the platform, including information about active workloads and configurations. If the platform finds that the engine's status has become outdated, it sends upgrade instructions or other maintenance updates to the engine. These instructions may upgrade the engine itself or update settings or workload versions. The engine automatically upgrades itself, then restarts. The log folder should also contain a SelfUpgrade log.

Platform Engine Management



Manual Platform Engine Update

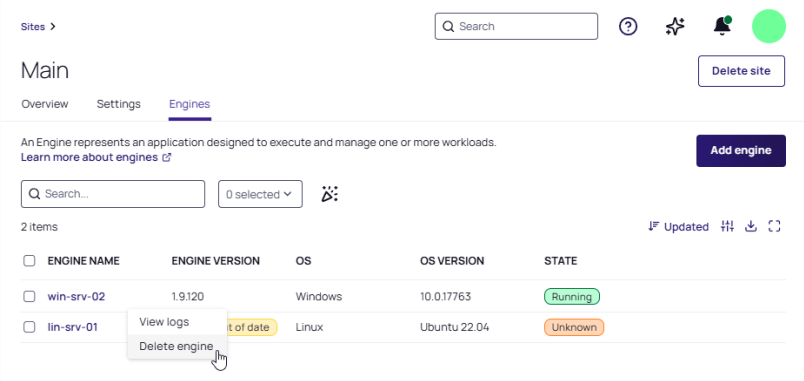
Beginning in Platform Engine version 1.5.8, automatic upgrades are supported. You should run a manual upgrade only if you are facing unknown exceptions.

To manually update the engine, follow the steps below.

1. Run the PowerShell script as described in "Manually Uninstall an Engine from Host Machine" on the next page.
2. Navigate to **Engine Management**.
3. Open the existing site.
4. Wait for the Engine to disappear from the engine list.
5. Once the old version of the engine disappears, click **Add Engine** to install the latest version of the engine.
6. Follow the steps in "Adding a Platform Engine" on page 246 to add the latest version of the engine.

Uninstalling an Engine from the Platform

Uninstalling the engine from the platform severs its association with the site and removes it from the site list.



1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Select the site where you want to delete an engine.
3. Click the **Engines** tab.

Platform Engine Management

4. Hover your cursor to the right of the engine name you want to delete
5. Click the ellipses that appears (...)
6. Click **Delete engine**.
7. Confirm your selection.

The platform then sends uninstall instructions to the chosen engine, which then automatically shuts itself down and uninstalls itself.

You can also delete engines using these procedures:

- Click anywhere in the row of the engine you want to delete, then click **Delete engine** from the preview panel that opens to the right.
- To delete engines in bulk, select the box to the left of the name of each engine you want to delete, then click **Delete engine**.

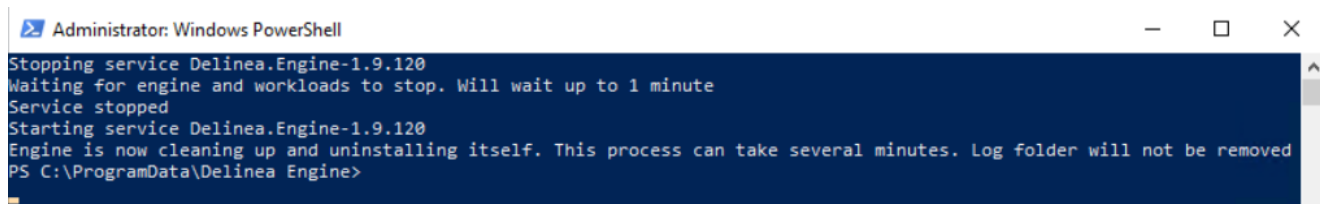
Manually Uninstall an Engine from Host Machine

To completely remove the engine from the Windows host machine, including all program files and installed ProgramData, execute the command below as an administrator.

windows Uninstall Script

```
cd "C:\Program Files\Delinea Engine\scripts";.\uninstall-engine-win.ps1;
```

Engine uninstall output:



```
Administrator: Windows PowerShell
Stopping service Delinea.Engine-1.9.120
Waiting for engine and workloads to stop. Will wait up to 1 minute
Service stopped
Starting service Delinea.Engine-1.9.120
Engine is now cleaning up and uninstalling itself. This process can take several minutes. Log folder will not be removed
PS C:\ProgramData\Delinea Engine>
```

To completely remove the engine from the Linux host machine, including all program files and installed ProgramData, execute the command below as an administrator.

Linux Uninstall Script

```
(InstallDir=`mktemp -d /tmp/delinea-engine-installer-xxxxxx`; trap "sudo rm -rf $InstallDir" 0 1 2 3 15; cd $InstallDir; echo "Downloading packages. This may take a moment..."; URL='https://enginepool-downloads-dev.azureedge.net/shell-installer/latest/linux-x64.tgz'; curl -fLO $URL; gunzip -c *.tgz | tar -xf -; sudo ./Delinea.EnginePool.Engine.Installer uninstall; sudo systemctl restart delinea-engine.service;)
```

Successful execution should yield a confirmation message indicating proper completion.

Windows Platform Engine and Log Directories

See "Local File Locations" on page 831

Linux Platform Engine and Log Directories

The Linux Platform Engine is installed at the following location:

- `/opt/delinea-engine/[version number]/`

Linux Platform Engine deployment files can be found in versioned folders at the location below. The versioned deployment folders are used for temporary processes, such as downloading and extracting deployment installations.

- `/var/delinea-engine/[version number]/`

Linux Platform Engine logs:

- `/var/delinea-engine/log`

The default log contains the following engine runtime information:

- Process logging
- Starting and stopping deployments
- Sending heartbeats to the platform

Platform Engine Log Levels

The current log levels for various components are found under **LogLevel** and **MinimumLevel** to the right of each component. These values can be changed to other values from the table below. Each level includes the levels below it. For example, if the level is set to **Warning**, messages at the **Error** level are also recorded.

Level	Description
Debug	High-volume logging for reporting detailed engine behavior
Information	Average-volume logging for normal engine function
Warning	Low-volume logging for unexpected but managed events
Error	Lowest-volume logging for undesired and unexpected events

The default logging levels provide a record of normal engine functions. If a different amount of logging is desired, all log levels should be changed to reflect the new desired level.

Adjusting Windows Platform Engine Log Levels

To change the engine log level, open the file at the following location in a text editor with administrator privileges:

- `C:\Program Files\Delinea Engine\[version-number]\`

Restart the Windows Platform Engine service using the Windows Services Manager.

Adjusting Linux Platform Engine Log Levels

To change the engine log level, open the file at the following location in a text editor with administrator privileges:

- `/opt/delinea-engine/[version number]/appsettings.json`

Restart the Linux Platform Engine service using `sudo systemctl restart delinea-engine.service`

Checking Logs in the Engine Management Interface

The logging page provides a comprehensive view of system logs, helping users to monitor and troubleshoot various components.



Note: Logs are retained for seven days, then they are automatically deleted from the database.

To check logs follow the steps below:

1. Click **Settings** from the left navigation menu, then click **Engine Management** from the secondary menu.
2. Click the name of a site where you want to add an engine.
3. Click the **Engines** tab.
4. Click the name of the engine with the log you want to check.
5. Click the **Logs** tab.

You can check logs of engines or logs of specific workloads by changing the value in the Source field.

[Learn more about logs.](#)

<input type="text" value="Search..."/>	Source Engine ▾ X	Level 0 selected ▾ X	Date All time ▾ X
50 items			
DATE ↓	SOURCE	LEVEL	MESSAGE
9/26/2024, 10:24:59 PM	Engine	Information	Msg Engine group: 696697b2-dcd4-4e95-b318-4d24da128ba5 - Delinea Privilege ...
9/26/2024, 10:19:59 PM	Engine	Information	Msg Engine group: 696697b2-dcd4-4e95-b318-4d24da128ba5 - Delinea Privilege ...
9/26/2024, 10:14:59 PM	Engine	Information	Local Engine group: 696697b2-dcd4-4e95-b318-4d24da128ba5 - Delinea Privilege...
9/26/2024, 10:09:59 PM	Engine	Information	Msg Engine group: 696697b2-dcd4-4e95-b318-4d24da128ba5 - Delinea Privilege ...
9/26/2024, 10:04:59 PM	Engine	Information	Msg Engine group: 696697b2-dcd4-4e95-b318-4d24da128ba5 - Delinea Privilege ...
9/26/2024, 9:59:59 PM	Engine	Information	Msg Engine group: 696697b2-dcd4-4e95-b318-4d24da128ba5 - Delinea Privilege ...

The logs table displays data in four columns: Date, Source, Level, and Message.

- **Date:** The date and time when the log entry was generated. Format: MM/DD/YYYY, HH:MM:SS. (US Eastern Time Zone)
- **Source:** Users can filter logs based on the origin of the log entry (Engine or a specific workload).

- **Level:** The severity or importance of the log entry. Different levels help users to prioritize and address issues accordingly.
 - **Trace:** Detailed information for tracing the execution of the system
 - **Debug:** Information useful for debugging purposes
 - **Information:** General information about system operations
 - **Warning:** Indicates a potential issue that may need attention
 - **Error:** Indicates that an error has occurred, requiring investigation
 - **Critical:** Represents a serious problem that requires immediate attention
- **Message:** Detailed information about the log entry, including context and specifics related to the log level.

For related content, see the following:

- [Engine Workloads](#)
- [Troubleshooting Platform Engine](#)

Understanding Engine Workloads

A workload is an application that runs a continuous task such as a background service.

Similar terms: payload, release

Each platform service or feature that uses Engine Management defines its own workloads. Engines carry out the execution of these workloads.

Workloads can have various versions, known as deployments. Deployments are similar to versions or editions of a workload. Each workload's engine runs a single deployment.

The following workloads run on the Delinea Platform Engine.

- "Audit Collector Workload" on page 257 (Windows)
Capability: Privilege Control for Servers
- "Command Relay Workload" on page 259 (Windows)
Capability: Privilege Control for Servers
- "PRA Workload" on page 263 (Windows and Linux)
Capability: Privileged Remote Access
- "ITP for Active Directory Workload" on page 266 (Windows)
Capability: ITP For Active Directory
- "AD Rapid Discovery Workload" on page 267 (Windows)
Capability: Privilege Control for Servers

Workload Deployment States

State	Description
Pending	The deployment has been accepted by the engine, but one or more of the entry points has not been set up and made ready to run. This includes the time the deployment spends waiting to be scheduled and the time the engine spends downloading packages over the network.
Running	The deployment has been bound to the engine, and all entry points have been created. At least one entry point is still running or is in the process of starting or restarting.
Succeeded	All entry points in the deployment have terminated with success, and will not be restarted.
Failed	All entry points in the deployment have terminated, and at least one entry point has terminated in failure. The entry point either exited with non-zero status or was terminated by the system.
Unknown	The state of the deployment could not be obtained. This state typically occurs due to an error in communicating with the engine where the deployment should be running.
None	The engine did not select this deployment to be run.

Workload Log Directories

See "Local File Locations" on page 831.

Monitoring Workloads

1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Select a site.
3. Click the **Engines** tab.
4. Select an engine.
5. Select the **Workloads** tab.

Overview

Workloads

Q Search...

States: 0 selected

1 item 1x Workload

WORKLOAD	VERSION	STATE
Delinea-Collector	6.01-343	Running
Delinea-Command-Relay	5.51-123	Running

Restarting Workloads

If you make changes to a workload, you must restart it to have the changes take effect.


WORKLOAD ↑	VERSION	STATE	MESSAGE
Delinea Audit Collector	6.11-319	Running	Collector running.
Delinea Command Relay	Restart workload	Running	Command Relay is running.
Delinea Privileged Remote Access	1.0.53-1725278906	Running	

1. Click inside the workload row near the right side of the WORKLOAD column.
2. Click the ellipsis.
3. Click **Restart workload**.

```
$zone = Get-CdmZone -Name "DelineaZone" Set-CdmDelegation -Zone $zone -Task "All" -Trustee "new_service_account@domain.test"
```

Audit Collector Workload

Audit collectors send audit data to the Delinea Platform, so recorded activities and events can be displayed. Audit Collectors function as intermediary services that receive and compress real-time activities captured by agents deployed on audited computers. Additional collectors can be deployed at any point for additional resiliency or improved scale.

 **Tip:** We recommend setting up at least two collectors to ensure uninterrupted auditing.

The agent on each audited machine captures user activities and forwards them to a designated collector. When the agent cannot establish a connection with a collector—such as when computers hosting the collector service are offline for maintenance—the agent temporarily stores the session data locally. When the connection is reestablished, the agent transfers this session data to the collector. The collector then transmits the data to the Delinea Platform.

Editing Audit Collector Settings

1. Open the **Engine management** settings page (use the Search bar to find it).
2. Select a site.
3. Select the **Settings** tab.
4. Click **Edit**.
5. Enable or disable Session Recordings to Platform, or change the port number.

Setting	Description
Send Session Recordings to Platform	When enabled, session recordings are sent from the collector to the platform for analysis and storage.
Port Number	5063 TCP is used by default. The Audit Collector listens on this port. Agents deployed on audited computers forward their captured user activities to the Audit Collector using this port.

Audit Collector Account Permissions

The permissions described in this section are needed only when you use the Audit Collector as a standalone workload, without the Command Relay, as when using Server Suite with the Delinea Platform. If you are using the Command Relay workload, it takes care of all the permissions that are needed.

For information about using Server Suite with the Delinea Platform, see ["Server Suite on Delinea Platform"](#) on page 806.

On the server where you will install the Delinea Platform Engine and the Audit Collector workload, define a service account for Audit Collector, then configure the account with local server permissions, domain permissions, or domain administrator permissions (temporary) as described in the next few sections.



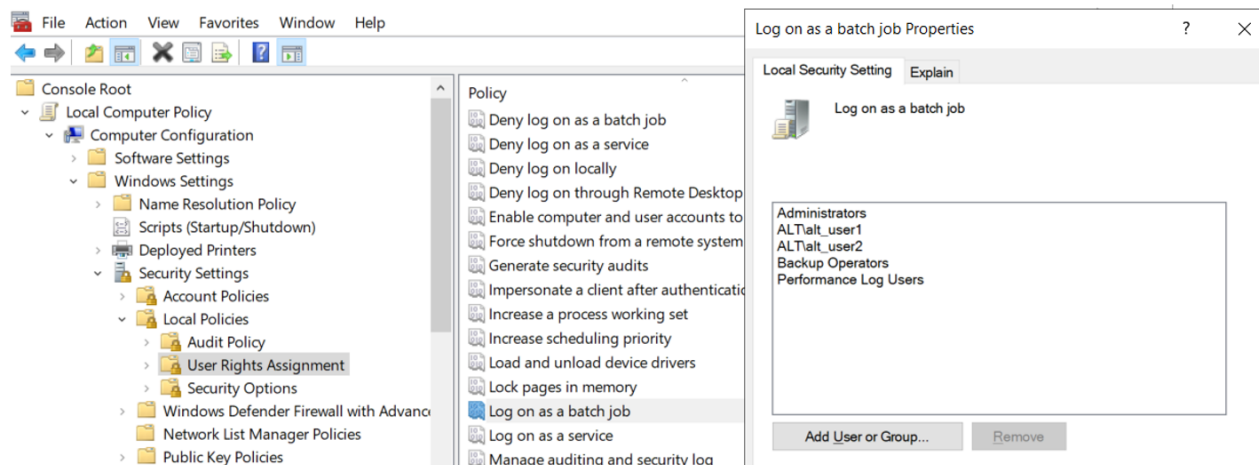
Note: If you do not want to grant any of your organization's users full control at the root level, create the DelineaPlatform OU and grant Delinea full control over it. Delinea then takes care of all child objects in the OU. At a minimum, you must grant Delinea read permissions at the root.

Local Server Permissions


With local permissions on the server where the Delinea Platform Engine and Audit Collector will be installed, the Audit Collector service account can create the DelineaPlatform OU manually before running the setup for Audit Collector. The local server permissions must include the **Log on as a batch job** permission in order for PCS to work.

To assign the Log on as batch job permission:

1. Select **Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.



2. Select the **Log on as a batch job** permission.
3. On the Local Security Setting tab, click **Add User or group**.
4. Navigate to and select the Audit Collector service account to apply the permission.

 **Note:** The **Log on as batch job** permission is granted by default to all members of these three AD groups:

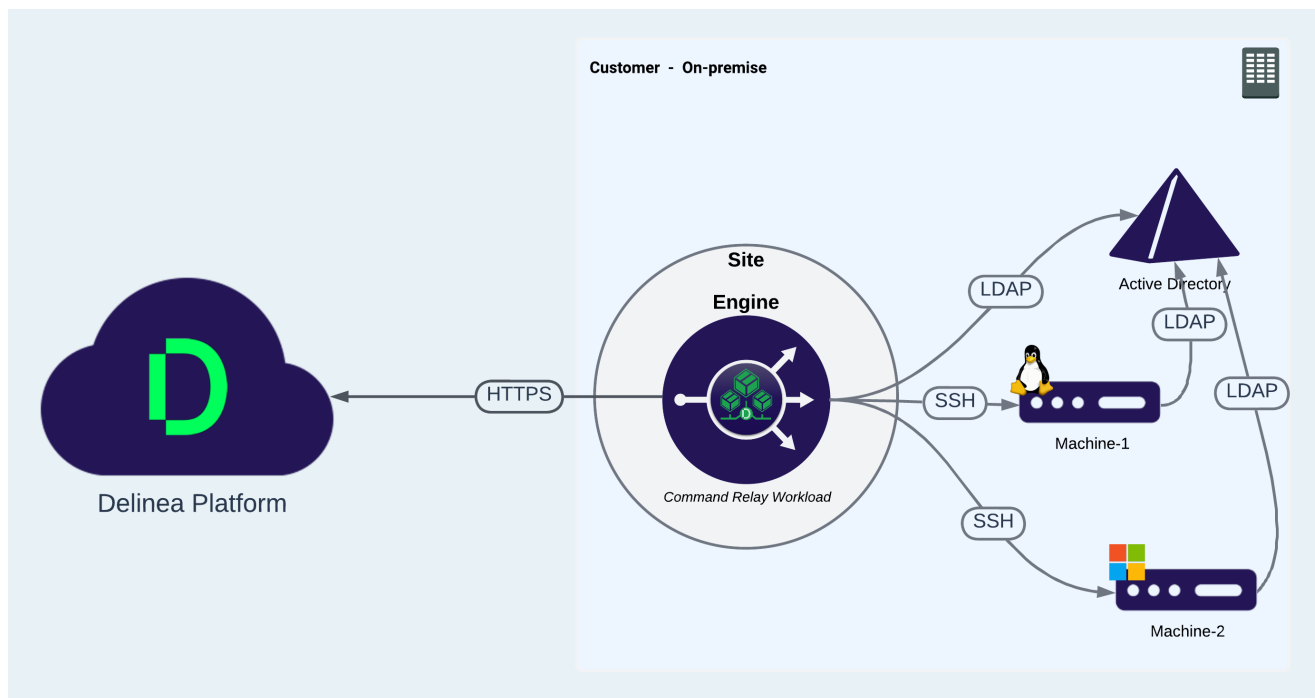
- Administrators
- Backup Operators
- Performance Log Users

Domain Permissions

An object named OU=DelineaPlatform must be created at the root of the domain. Permissions giving Full Control to create the OU=DelineaPlatform object and all child objects must be given to the Audit Collector service account. In the Permissions section of the Permission Entry dialog, every checkbox must be selected.

Command Relay Workload

The command relay workload is a service that facilitates communication between the customer and the Delinea Platform through an SSH connection. Its primary function is to dispatch commands along with their parameters to be executed within the customer's environment. The command relay requires a service account that can modify your domain so the proper administrative policies can be added.



Command Relay Prerequisites

.Net 4.8 - must be installed on the Delinea Platform Engine target machine.



Note: If .Net 4.8 is not already installed, Command Relay installs it automatically. In this case, you need to reboot the server.

Command Relay activates the PowerShell module on the Windows Server machine, and it downloads and installs the PowerShell feature required by Command Relay.

Editing Command Relay Settings

To execute the Command Relay workload, a Command Relay Service account must be selected. Follow the steps below to add the account. The user will only see accounts for which they have permissions.

1. Click **Settings** from the left navigation menu, then click **Engine Management**.
2. Select a site.
3. Click the **Settings** tab.
4. Next to Delinea Command Relay, click **Edit**.

The first time this settings page is opened, the Command Relay Service Account shows **None**.

5. Click **Select**.
6. Search for the vaulted account where you have permissions, and select the account.
 - The logged-in user must be the owner of the secret for the account.
 - The secret must not be configured for checkout.

7. Select **Turn off folder inheritance and Share Secret**. This disables inheritance, granting workloads access to the secrets.
8. Click **Save** after the domain is selected.

Setting	Description
Domain	User should be able to select the Domain accounts they already have access to

Command Relay Account Permissions

On the server where you will install the Delinea Platform Engine and the Command Relay workload, define a service account for Command Relay, then configure the account with **local server permissions**, **domain permissions**, or **domain administrator permissions** (temporary) as described in those sections below.

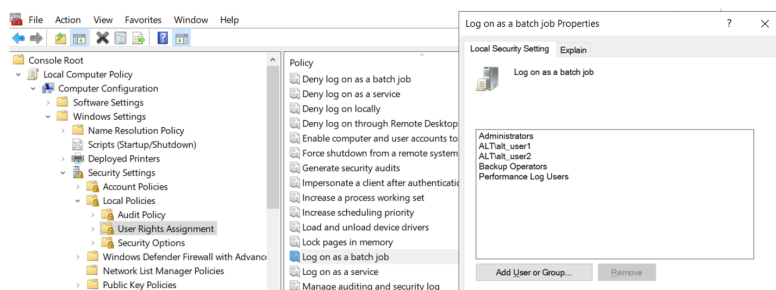
Local Server Permissions

With local permissions on the server where the Delinea Platform Engine and Command Relay will be installed, the Command Relay service account can create the DelineaPlatform OU manually before running the setup for Command Relay. The local server permissions must include the **Log on as a batch job** permission to allow PCS to work.

Assign the Log on as batch job permission

To assign the **Log on as a batch job** permission to the Command Relay service account, follow these steps:

1. Select **Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.



2. Select the **Log on as a batch job** permission.
3. On the Local Security Setting tab, click **Add User or group**.
4. Navigate to and select the Command Relay service account to apply the permission.

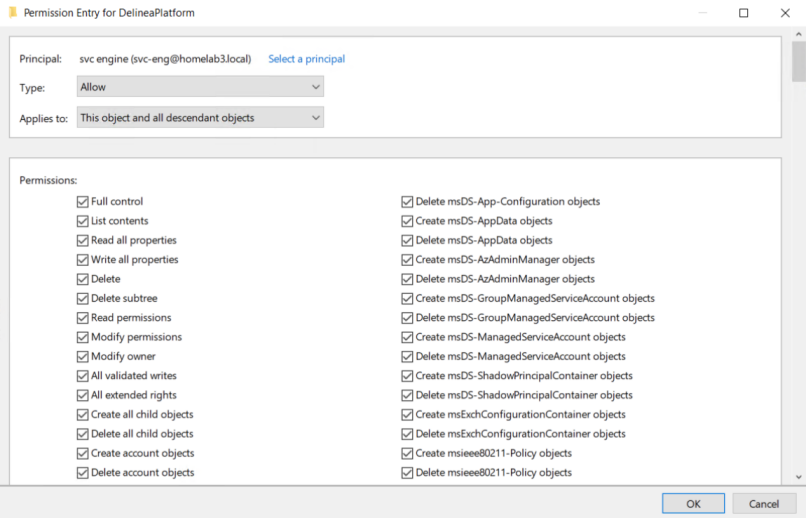


Note: The **Log on as batch job** permission is granted by default to all members of these three AD groups:

- Administrators
- Backup Operators
- Performance Log Users

Domain Permissions

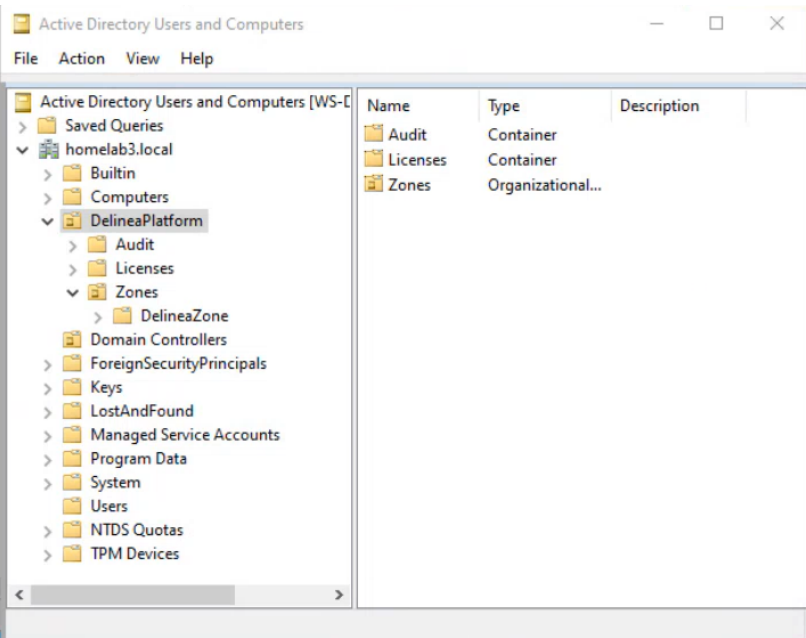
An object named OU=DelineaPlatform must be created at the root of the domain. Permissions giving Full Control to create the OU=DelineaPlatform object and all child objects must be given to the Command Relay service account. In the Permissions section of the Permission Entry dialog, every checkbox must be selected, as shown in the following image.



The DelineaZone

When Command Relay executes, it creates the DelineaZone within the DelineaPlatform OU, as shown in the following image.

The DelineaZone contains all the agent policies that need to be enforced on applicable servers. The DelineaZone is managed by the platform.



Minimum Permissions to Join a Server to a Zone

The minimum permissions required to join a server to the DelineaZone depend on the operating system.

Windows

The minimum permissions for an AD user or group to join a Windows server to the DelineaZone:

- Local Administrator permissions on the server
- AD Permissions:
 - Create all child objects
 - Generic Read

***nix**

The minimum permissions for an AD user or group to join a *nix server to the DelineaZone:

- Root permissions on the server
- AD Permissions: Create AD Computer Object
- AD Permissions: DelineaZone:
 - Create all child objects
 - Generic read

Switching Command Relay Service Accounts

On the server where you will install the Delinea Engine and the Command Relay workload, you can define more than one service account for Command Relay. To use another service account for Command Relay, you must delegate the zone permissions to the new service account. To do so, run the following PowerShell script on the Command Relay machine (substitute your own value for `new_service_account`). You must be logged in as a user with sufficient privileges to modify the zone:


PRA Workload

Delinea Privileged Remote Access (PRA) provides seamless access to remote machines through RDP (Remote Desktop Protocol) and SSH (Secure Socket Shell) without the need for a VPN (Virtual Private Network).

Delinea PRA runs on the Delinea Platform and seamlessly integrates with Delinea Secret Server vault, deployed from the cloud or from within a customer's private network. PRA automatically uses credentials to connect with target resources, enabling RDP and SSH connectivity as well as SMB and SFTP file transfers without exposing sensitive parts of credentials to the end-user. This fast and simple workflow is completely integrated into the Delinea Platform user interface.

When a user requests a connection to a remote target, they connect to the Delinea Platform first with their browser. If authorized, the Delinea PRA workload facilitates the connection with the target machine. The PRA workload is also used to integrate Secret Server On Premise installations with the Delinea Platform.

The PRA workload works for both Windows and Linux.

 **Important:** Before employing the PRA workload, please be sure you are familiar with the content at [Platform Engine Management](#) and [Understanding Engine Workloads](#).



When a site has multiple engines or workloads, PRA automatically selects an engine or a workload to make the remote connection. During the preview phase, if the Engine Management Site with available Windows workloads has the same name as a PRA site with available Linux engines, PRA considers all available Windows and Linux options before making a selection.

Sizing for the PRA Workload

This document offers guidance to users to determine what hardware configuration is needed to host the PRA workload depending on the number of concurrent PRA session that engine needs to host.

Size testing was performed on Platform Engine hosts equipped with an Intel(R) Xeon(R) Gold 6254 CPU @ 3.10GHz 3.09 GHz processor, 64-bit operating system, x64-based processor and with 6GB of RAM.

Sessions were tested on a site with a single Platform engine with PRA capabilities. No other capabilities were added to the engine.

Multiple concurrent sessions were opened, kept running for 30 minutes and then closed. The following actions were performed on the remote target machines after connection was established:

1. SSH: Login to a remote Linux server and run “top”.
2. RDP: Login to a remote Windows server and run a batch script that produces output similar to that of a typical command-shell script.

Session recording was disabled in both test cases.

Session Type	# of PRA Workloads	# of Concurrent Sessions	CPU Usage %	Memory Usage in MB
SSH	1	200	0.357 avg (8.921 max)	13.21 avg (13.21 max)
RDP	1	100	0.706 avg (24.297 max)	13.54 avg (16.21 max)

Your actual capacity may vary depending on the specific activities that are being carried out on the remote target machine. For example, viewing a video clip on the remote machine on RDP will put very different load on PRA as compared to running *vim* to edit a text file on a remote SSH session. Performance test data also indicates that PRA performance is more dependent on memory and bandwidth than CPU speed or power.

The network latency between the end-user’s browser and the Delinea Platform, or the latency between the Platform Engine and the target server also affects the user-experience.

We recommend the following steps when experiencing PRA performance issues that may be associated with the Engine:

1. Use system monitoring tools to determine whether any specific resource like memory, network bandwidth, CPU utilization is running at unacceptably high levels. If possible, increase the corresponding hardware or virtualization resources.
2. Deploy more engines to the parent site.
3. Check the network latency between:
 - a. The Engine and the Delinea Platform tenant.
 - b. The Engine and target machines
4. Contact Delinea Support.

Troubleshooting the PRA Workload

This page gives information about how to investigate and solve issues with the PRA workload.

PRA Workload Log File Locations

The PRA workload log files can be found in the following locations:

- Windows:

C:\ProgramData\Delinea Engine\log

- Linux:

/var/delinea-engine/log



Note: When checking the log files for both Windows and Linux, it is important that you look at the file that begins with *remote-access-service*. For example: *remote-access-service_1.0.67-1729865933_20241112.log* where:

- *1.0.67-1729865933* is the PRA workload version
- *20241112* is the date

In some cases, you may need to look at logs on the remote target system being accessed, for example Windows Event Viewer which would contain logs related to possible errors with Windows remote access services, authentication, etc. Some examples include:

- [Auditing Remote Desktop events](#)
- [Auditing Kerberos events](#)

PRA Workloads Displayed as "Offline" in the UI

If PRA workloads are displayed as "Offline" in the UI, check to see if you have set a static UUID. See "[Setting a Static UUID](#)" on page 364 for more information.

Troubleshooting Proxy Issues

If you are experiencing issues connecting to the target machine through a secret with proxy enabled, collect the proxy logs to assist the Delinea Support team with troubleshooting. For more information about collecting proxy logs, refer to the [Secret Server documentation](#).

ITP for Active Directory Workload



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

The ITP for Active Directory workload for Windows fetches Active Directory identity data about users, groups, service accounts, memberships, and user ACLs to provide a full picture about the accounts and their permissions, identifying admins, shadow admins, and AD misconfigurations that can lead to unsecured accounts, and helping you to quickly vault privileged accounts. The workload is used to integrate Active Directory identity data for the platform features listed below. Click the links to learn how privileged accounts are evaluated, discovered, and vaulted:

- "Continuous Identity Discovery" on page 738
- "ITP and PCCE" on page 677

Prerequisites

- .Net 8 installed on the Delinea Platform Engine target machine
- Licensing for the Continuous Identity Discovery feature of Delinea Platform

Adding ITP for Active Directory

1. From the left navigation menu click **Settings**, then click **Engine Management**.
2. On the Engine management page, select a **Site**. If no site exists, create a new site and select it.
3. Select the **Engines** tab
4. Select an engine. If no engine exists, create a new engine and select it.
5. Select the **Capabilities** tab.
6. On the Capabilities page, select **Add Capabilities**.
7. Select the box next to **ITP for Active Directory**.
8. Click **Add**.

Editing ITP for Active Directory

To run the ITP for AD workload, you must select an AD account with read access. Follow the steps below to add the account. The user will see only the secrets for which they have permissions.

Platform Engine Management

1. From the left navigation menu click **Settings**, then click **Engine Management**.
2. Select a site.
3. Click the **Settings** tab. The first time this settings page is opened, the Platform Engine ITP for Active Directory service account shows *None*.
4. Next to **ITP for Active Directory**, click **Edit**.
5. Next to **Active directory credentials**, click **Select**.

Platform Engine ITP For Active directory

Edit

[Learn more about Platform Engine ITP For Active directory](#) 

Active directory credentials —

Select

Cancel

Save

6. On the **Share secret with Delinea Workload** page, select **All secrets**.
7. Search for a secret that you own.
8. Select the secret.
9. Make sure the secret is not configured for checkout.
10. Select **Turn off folder inheritance and Share Secret**. This disables inheritance, granting workloads access to the secrets.
11. Click **Save**.

AD Rapid Discovery Workload



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

AD Rapid Discovery maintains continuous synchronization between Active Directory (AD) and the Delinea Platform. The Windows Server Manager can be used to change computer properties within AD. Any changes made to computers in AD trigger real-time synchronization through AD Rapid Discovery to the Server Suite Agent, and the changes appear on the Delinea Platform. Changes to the computer where AD Rapid Discovery is running appear in the Inventory page of the platform after synchronization.

The default synchronization frequency is every five minutes. You can configure the synchronization frequency.

Deployment

The AD Rapid Discovery workload can be installed and run on any domain joined machine. This page gives details about how to set up the workload.

Editing AD Rapid Discovery Settings

To execute the AD Rapid Discovery workload, a Service account must be selected. Use the following steps to add the account. You will only see accounts for which you have permissions.

You can also use these steps to adjust the refresh interval.

1. Open the **Engine management** page (use the Search bar to find it).
2. Select a site.
3. Click the **Settings** tab.
4. In AD Rapid Discovery, click **Edit**.
5. You can make the following settings:
 - AD Rapid Discovery Domain Admin Account: This account is used to run AD Rapid Discovery.
 - Type a new value for the frequency at which AD Rapid Discovery synchronizes with AD, and click **Save**.

Setting	Description
AD Rapid Discovery Domain Admin Account	This account is used to run AD Rapid Discovery. You can use a Domain Admin Account or an AD account that has the permissions described later in this page, in "Setting AD Rapid Discovery Account Permissions" below.
Synchronizes with AD	Time interval (in minutes) between times when the AD Rapid Discovery workload uploads any new data from AD to the platform.

Setting AD Rapid Discovery Account Permissions

On the server where you will install the AD Rapid Discovery workload, define a service account for AD Rapid Discovery, then configure the account with local server permissions and domain permissions.

Local Server Permissions

With local permissions on the server where the AD Rapid Discovery workload will be installed, the AD Rapid Discovery service account can run the setup for AD Rapid Discovery.

The local server permissions must include the **Log on as a batch job** permission and the **Log on as a service** permission.

To assign the required logon permissions:

1. Select **Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment**.
2. Select the **Log on as a batch job** permission and the **Log on as a service** permission.
3. On the Local Security Setting tab, click **Add User or group**.
4. Navigate to and select the AD Rapid Discovery service account to apply the permissions.

Domain Permissions

The AD Rapid Discovery workload requires the AD permission **Replicating Directory Changes**. This permission must be granted to the AD Rapid Discovery service account on the root domain node.

In the Permissions section of the Windows Permission Entry dialog, select the checkbox for Replicating Directory Changes.

Troubleshooting Platform Engine

This page contains information to help you diagnose and fix issues related to the Delinea Engine.

Engine Doesn't Appear, is Outdated, or Status Shows “Failed”

Investigate engine-specific logs here:

C:\ProgramData\Delinea Engine\log\

- Delinea.Engine.Registration.[date].log
 - Contains registration process logging
- Delinea.Engine.Bootstrap.[date].log
 - Contains startup flow logic logging
- Delinea.Engine.Default.[date].log
 - Contains runtime and communication logging

Engine Upgrade Problems



Note: Beginning with Delinea Engine version 1.4.3, if you have an existing installed engine, the engine recognizes when updates are available and upgrades itself automatically. Manual upgrades are no longer necessary.

Check this path for engine-specific logs: C:\ProgramData\Delinea Engine\log\

If Delinea.Engine.SelfUpgrade.[date].log exists in this folder, the engine has begun an upgrade attempt. This process can take several minutes, and the logs may include error messages as the deployments are shut down for the upgrade. Engine heartbeats occur at five-minute intervals, and it might take some time for Engine Management to recognize that the engine has been updated.

If issues are encountered during upgrade or the engine still appears outdated in the UI, try a manual reinstall using the steps in the next section.

Need to Manually Reinstall Engine

1. Open PowerShell ISE or Powershell.exe as administrator and run the script as described in ["Manually Uninstall an Engine from Host Machine"](#) on page 252.
2. Ensure that the result does not report any errors, and looks similar to the following output:
[08:19:08 INF] BeginUninstallFlow [08:19:08 INF] Version: {VERSION}
3. Wait for the engine to uninstall.

4. Log in to your Delinea Platform.
5. From the left navigation menu, click **Settings**, then click **Engine Management** from the secondary menu , and make sure the engine disappears.
6. Select the site for the engine you are reinstalling.
7. Click **Add Engine** and copy the full Quick Install script.
8. Run the script in PowerShell ISE or Powershell.exe as administrator.

Workload Status Shows “Failed”

Check the log files. See "[Local File Locations](#)" on page 831.

PRA Workload: PRA Workload log file paths:

■ Windows:

C: ProgramData\Delinea Engine\log\remote-access-service_[version-number].log

■ Linux:

/var/delinea-engine/log



Note: When checking the log files for both Windows and Linux, it is important that you look at the file that begins with *remote-access-service*. For example: *remote-access-service_1.0.67-1729865933_20241112.log* where:

- *1.0.67-1729865933* is the PRA workload version
- *20241112* is the date

Getting 400s When Engine is Trying to Register

1. Verify that time in domain is accurate. If the time in the domain is a few minutes off, the ntp service on hosts isn't running.
2. Reconfigure the ntp service and sync the domain controller.

Engine and Logs Directory Structure

After installation and registration of the Platform Engine, the following folder is created:

C:\ProgramData\Delinea Engine\[version number]\

This folder contains the sub-folders described in this table:

Folder	Description
\appdata	Contains key file used to encrypt configuration files to discourage manual, machine-level changes.

Folder	Description
\appdata\settings	Contains encrypted engine configuration files: engine options, deployments, connections, and upgrade/uninstall configuration files when relevant.
\runtime\delinea\<deployment name>\<version>	Contains folders for the installation of deployments. The contents of these folders should not be manually edited.
\metadata	Contains information used to verify the integrity of deployment installations. Contents of this directory must not be modified.
\deployment\delinea\<deployment name>\<version>	Contains a versioned folder for each deployment used for temporary processes such as downloading and extracting deployment installations. Each versioned folder contains a settings folder and a deployment state encryption key.
C:\ProgramData\Delinea Engine\log	<p>Contains engine runtime logs.</p> <p>Contains Precheck, Bootstrap, Registration, and Default logs. Precheck logs identify requirements and record any issues early. Bootstrap and Registration logs record engine startup and registration.</p> <p>Default log contains process logging, including updates from the platform's Engine Management service, starting and ending deployments, and sending heartbeats to the platform.</p> <p>This folder might also contain a SelfUpgrade log that records when the engine starts, detects a new version, and installs the new version. If the engine detects an Uninstall configuration file, it automatically shuts down and uninstalls itself. It also contains logs for each deployment.</p>

Active Directory Connector

Many users connect Active Directories to the Delinea Platform. What makes this possible is implementation of the Delinea Active Directory Connector. The Connector enables secure communication between the Delinea Platform and Active Directories (AD).

Determining Whether You Need the Delinea Connector

The Delinea Connector is a versatile application that ensures secure interactions between various services within your internal network and your platform tenant. The installation of at least one connector is necessary under any of the following conditions:

- You intend to use Active Directory as the identity repository for authenticating users on the Delinea Platform.
- You consider [Configuring IWA](#) to be an adequate method for Active Directory user accounts to access the platform.
- You wish to prompt users for [RADIUS Authentication](#), allowing your RADIUS server to verify users on the Delinea Platform. In this scenario, the Delinea Connector functions as a RADIUS client.
- You are considering using [Privilege Control for Servers](#).

For enhanced reliability and efficiency, we recommend deploying multiple connectors to enable failover capabilities and load distribution.

Related Content:

- [Using Connector Best Practices](#)
- [Installing the Delinea Connector](#)
- [Troubleshooting the Delinea Connector](#)

Installing the Delinea Connector

This topic explains how to install the Delinea Connector. Be sure you have first met the server requirements in the next section.

Server Requirements

The following list describes the requirements for the server or virtual machine where the Delinea Connector is installed:

- Always running and accessible on the internal network.
- Running Windows Server 2019 or newer.
- Running in 64-bit mode with 8 GB of memory or more, of which 4 GB or more must be available for connector cache functions.
- Running Microsoft .NET version 4.8 or newer. If it isn't already installed, the connector installer installs it for you. In this case, you must manually restart your machine to complete installation.
- If the connector is integrating with an on-premises Active Directory, the machine where it is installed must be joined to Active Directory to use as the identity store.

- Set up for outbound Internet access on port 443 (no Internet-facing ingress ports are required). For details on the connector's network requirements, see [Delinea Connector](#). Use of deep packet inspection filtering of HTTPS or SSL traffic by web proxies or security software may cause connectivity issues. In all cases, the ports and addresses discussed should be excluded from packet inspection to allow for normal service operation.

Set up for outbound Internet access on port 443 (no Internet-facing ingress ports are required). For details on the connector's network requirements, see "Delinea Connector" on page 84. Use of deep packet inspection filtering of HTTPS or SSL traffic by web proxies or security software may cause connectivity issues. In all cases, the ports and addresses discussed should be excluded from packet inspection to allow for normal service operation.

- If your network is configured with a web proxy server that you want to use to connect to the platform, you must specify this server during the installation process, and the web proxy server must support HTTP1.1 chunked encoding.
- As a best practice, avoid installing the connector on a domain controller.

Account Permission Requirements

This section details the permissions required for installing the Delinea Connector including Platform, Connector, Connector security, alternate accounts and OUs, and read access permissions.

Platform Permissions

To generate a connector registration code or manage the connector settings, you must belong to the Administrator group on the Delinea Platform.

Delinea Connector Permissions

You must be a local administrator on the machine where you are installing Delinea Connector, so that you can copy files to Program Files, set up a Windows service, and make registry settings.

Connector Security Permissions

The machine where the Connector is installed should have user access and other permissions assigned the same way they are assigned to an Active Directory domain controller. Access to the registry on the Connector machine should be appropriately restricted, and not available to all users.

Alternate Accounts and Organizational Units Permissions

You can run the Delinea Connector service as an Active Directory service account or as a Local System account. Make sure you have set up all permissions required for the account type you choose. For example, if you run the connector service as a specific Active Directory service account, the account must have the following characteristics:

- Member of the local Administrators group
- Read permission (at least) to the container, with platform user accounts and Active Directory Groups used as members of platform groups
- Read permission to the root DSE to gather necessary topology information

You should not run a Windows service with an Active Directory built-in account or an Active Directory user account.

You must verify that the relevant accounts have permission to read Active Directory users and groups as if authentication would work. Each time role permissions are reassessed, the connector tries to resolve the Active Directory groups mapped to any role in which the Active Directory user is potentially a member.

The computer account of the server where the connector is installed must also have read access to the container or organizational unit (OU) that stores the user accounts. Without read access, the connector cannot authenticate the user. Domain computers have this permission by default; however, the connector machine might not. This most often occurs in multi-forest or multi-domain setups, and can occur even when two-way trust is already defined. You can tell when this occurs, because the connector log shows the error message "Unable to locate forest or user object." In this case, you need to give the Local System account read access permission to the containers or organizational units.

Setting Read Access Permission to the User Account Container or Organizational Unit

1. Open Active Directory Users and Computers.
2. Select the user account container and open the **Properties**.
3. Select the **Security** tab.
4. Click **Add** to add the user account you are using to run the connector service.
5. Click **OK** after you add the user account.
6. Click the user account in **Group or User Names** and select the **Allow** checkbox for the **Read** permission.
7. Click **OK**.

Any user or group with permissions to read and write the LockoutTime attribute for an OU or other container can unlock user accounts that reside in that container.

Setting Read Access Permission to User Account Container with Powershell

Requirements

- Account with Domain Admin credentials
- Dcls.exe - This is installed on all Domain Controllers and can be installed on Member servers as part of the Delinea Connector deployment.
- Elevated PowerShell shell

Step 1: Run the following test command from an elevated PowerShell session under Domain Admin credentials. This command returns the current permissions to the folder you need access to.

```
dsacl "CN=Deleted Objects,DC=delineacloud,DC=com" /takeownership
```

This example domain is `delineacloud.com`. Replace the `delineacloud` and `com` with the FQDN of your domain.

If the test command succeeds, the output looks similar to what appears in the following screen shot (these are the initial settings for this folder on a Windows 2022 Server).

Active Directory Connector

DacIs.exe - This is installed on all Domain Controllers and can be installed on Member servers as part of the Delinea Connector deployment.

```
PS C:\Windows\system32> dsacIs "CN=Deleted Objects,DC=delineacloud,DC=com" /takeownership
Owner: dcloud\Domain Admins
Group: NT AUTHORITY\SYSTEM

Access list:
{This object is protected from inheriting permissions from the parent}
Allow dcloud\PLATFORM-PDC-01$ SPECIAL ACCESS
LIST CONTENTS
READ PROPERTY
Allow BUILTIN\Administrators SPECIAL ACCESS
LIST CONTENTS
READ PROPERTY
Allow NT AUTHORITY\SYSTEM SPECIAL ACCESS
DELETE
READ PERMISSIONS
WRITE PERMISSIONS
CHANGE OWNERSHIP
CREATE CHILD
DELETE CHILD
LIST CONTENTS
WRITE SELF
WRITE PROPERTY
READ PROPERTY

The command completed successfully
```

Step 2: At the PowerShell prompt, enter the following command:

```
dsacIs "CN=Deleted Objects,DC=delineacloud,DC=com" /g dcloud\adsync:LCRP
```

This command applies the user level account (not a Domain Admin) dcloud\adsync from the delineacloud.com domain to the folder.

Troubleshooting: If you run this command under Domain Admin credentials, and you get an INSUFF_ACCESS_RIGHTS error, the default settings for this container have been altered.

```
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32>dsacIs "CN=Deleted Objects,DC=commercial,DC=local" /g commercial\PAM-AD-Sync-SA:LCRP

Specified operation failed with ldap error:
00000005: SecErr: DSID-03152E29, problem 4003 (INSUFF_ACCESS_RIGHTS), data 0

Insufficient Rights
Access is denied.
The command failed to complete successfully.

C:\Windows\system32>
```

The workaround is to temporarily place the account with the Domain Admin credentials in the domain Builtin\Administrators group. Once that is done, run steps 1 and 2 again.

External References

- [How to let non-administrators view the Active Directory deleted objects container](#)
- [Install RSAT on Windows Server](#)

Downloading the Delinea Connector and Getting a Registration Code

To download the Delinea Connector:

Active Directory Connector

1. Log in to the Delinea Platform.
2. From the left navigation, select **Settings**, then select **Connectors**.
3. Click **Add connector**.
4. On the **Add connector** page, download the connector installation package.
5. Copy the tenant URL and save it for use during the connector installation process.
6. Create a new registration code or copy an existing one and save it for use during the connector installation process.

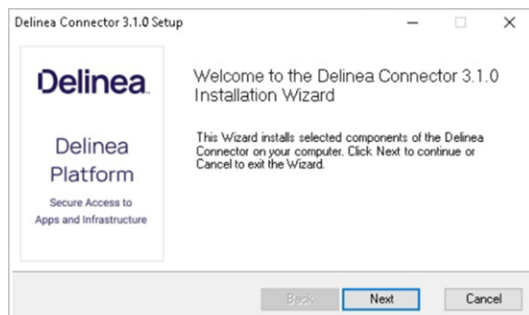


Note: The auto-generated registration code is created with default values only. It does not have an expiration time or limits on how many times the registration code should be used.

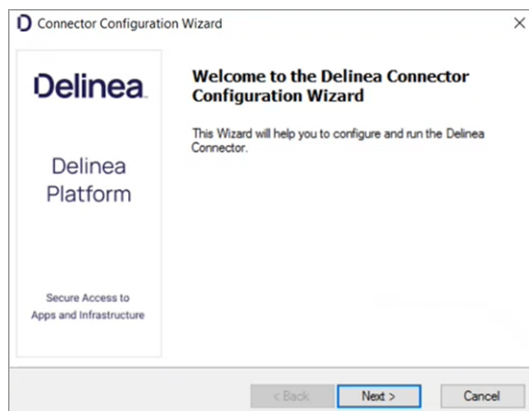
Installing and Configuring the Delinea Connector

To install and configure the Connector:

1. On the *Delinea Connector machine*, run the connector Installer file you downloaded in the previous section. The connector Installation Wizard opens.



2. Click **Next**.
3. Select the **Connector** tab.
4. Click **Register**. The Connector Configuration Wizard opens.





During the configuration process, we recommend keeping default settings, except where these instructions indicate otherwise. You can choose to configure the connector to change TLS to 1.2 for every .net app on the machine globally.

5. Click **Next**.
6. Select the **Enable strong encryption protocols system-wide** checkbox.
7. If you are using a web proxy server to connect to the platform, select the **Use a web proxy server for the Delinea Platform connection** checkbox. Specify the **IP Address**, **Port**, **User name**, and **Password**.

8. Click **Next**.

9. In the **Tenant URL** field, paste the tenant URL you copied and saved earlier.
10. Select the **Temporarily add Tenant URL to [browser's] trusted sites list** checkbox.

11. Select the **Use Registration Code** checkbox.
12. Paste the registration code you copied and saved earlier into the **Use Registration Code** field.
13. (Optional) You must be the domain administrator of the Active Directory domain for the relevant deleted objects container. If you are deleting users in multiple domains, make sure you are the domain administrator for all those domains. If you wish to enable the synchronization of user deletions in Active Directory with the Delinea Platform, follow these instructions:
 - Choose the domain(s) you wish to monitor and provide the required credentials for permission assignment.
 - Essential: grant the connector read access to the deleted objects container. You can provide the necessary permission by running the following commands on each connector:
 - If you do not already have the necessary permissions to change the permissions of the deleted objects container, run this command:

```
dsacl /s "CN=Deleted Objects,DC=<EXAMPLE>,DC=<COM>" /takeownership
```
 - The following command grants the Delinea Connector permission to read the deleted objects container in Active Directory:

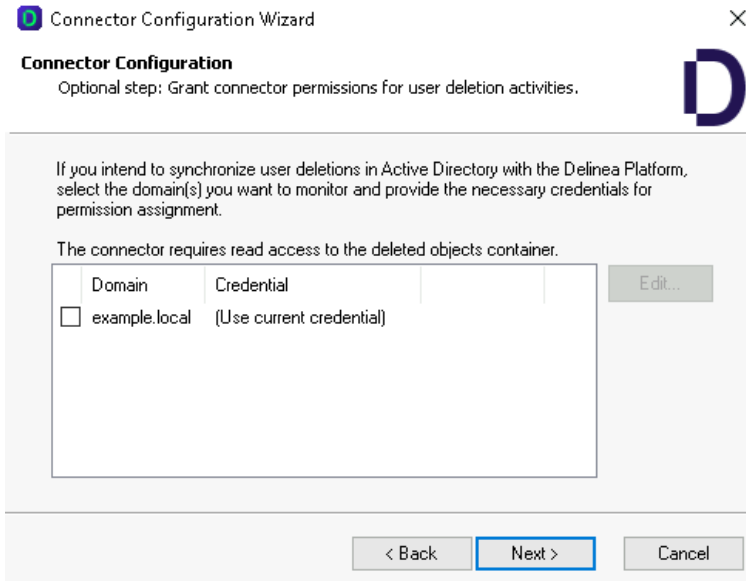
```
dsacl /s "CN=Deleted Objects,DC=<EXAMPLE>,DC=<COM>"  
/user:administrator@<EXAMPLE.COM> /passwd:* /g  
\\<EXAMPLE>\\<MACHINE_NAME>\\$<LCRP> /I:T
```

If this command fails, the default settings for this container have been altered. The workaround is to temporarily place the account with the Domain Admin credentials in the domain Builtin\Administrators group, then run the steps again.

Apply read permissions to the service account for the deleted objects container in the corresponding domain.



If you fail to perform any of these actions, users deleted in Active Directory will still be listed on the Users page in the Delinea Platform until you manually remove them. However, these users will not have access to any platform functionality.



14. Click **Next**.

The wizard performs checks to validate the network environment. Wait for the checks to complete.

15. Click **Next**.

The screen displays a bar indicating the progress of the configuration. Wait for the bar to be full.

16. Click **Next**.

You should see a notice saying, "Connector setup is complete."

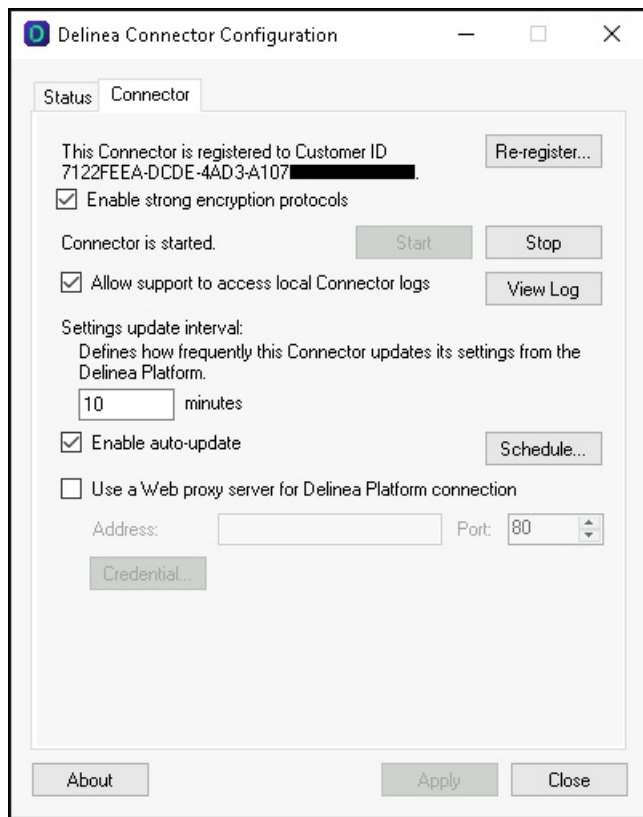
17. Click **Finish**.

Enabling Auto-Update for the Delinea Connector

You can configure the connector to automatically poll the Delinea Platform for software updates and install them. If an update is available, the connector downloads and installs the update, then restarts. The connector is enabled to poll automatically by default. You can also specify the auto-update time windows as needed.

Active Directory Connector

1. Log in to the Delinea Connector server.



2. Open the Windows Start menu and start the Delinea Connector Configuration program.
3. Select the **Enable auto-update** checkbox to enable automatic updates.
4. In *Enable auto-update*, click **Schedule** to configure the auto-update time window.
5. Click **Apply**.

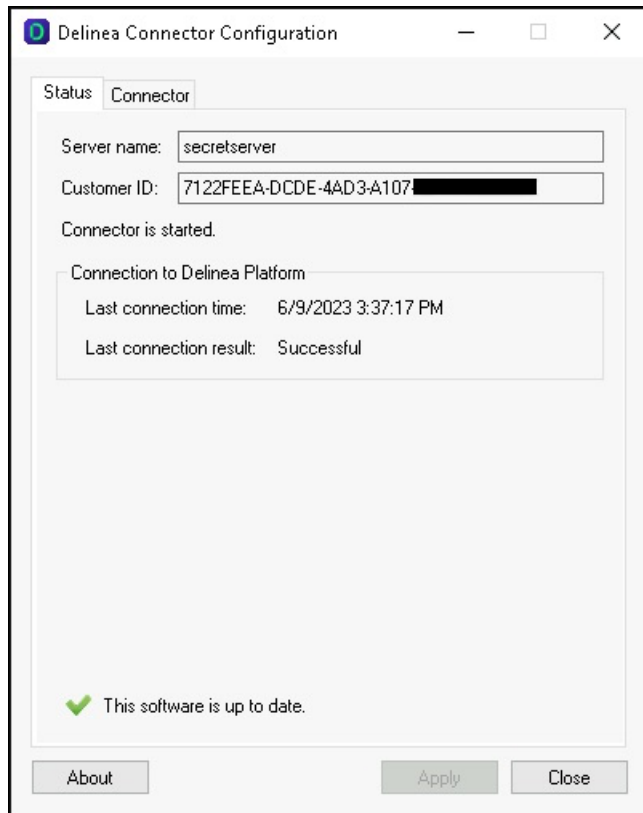
Updating the Delinea Connector

To update the Delinea Connector:

1. Open the Windows Start menu and start the Delinea Connector Configuration program.
2. In the lower left of the **Status** tab, right-click the update icon and select **Update**.

Active Directory Connector

The connector updates and displays a message indicating that the software is up to date.



Checking the Delinea Connector Status

To verify the status of the connector, click **Ping connector**.

If all components are functioning correctly, a success banner displays the message *Ping to connector was successful*. If any communication issues are detected between the platform and the connector, an error message is displayed. The timestamp for the last ping is updated to reflect the most recent successful ping check.

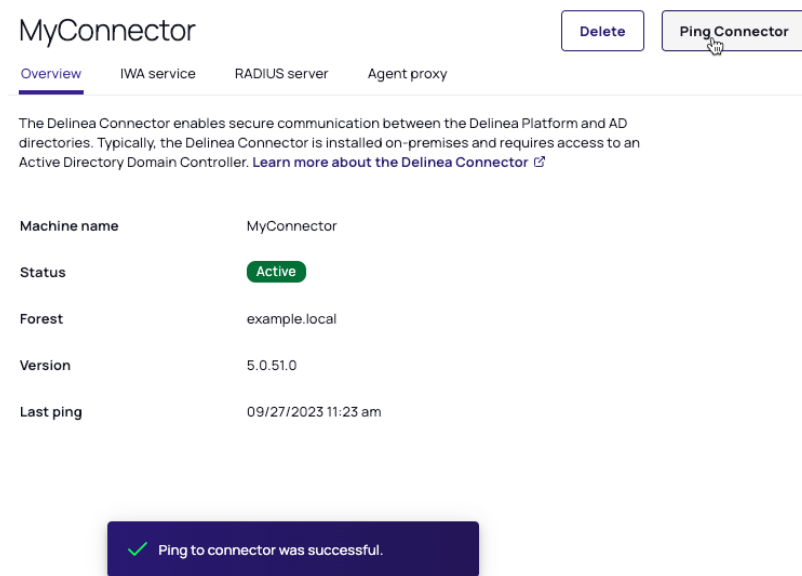
To download the Delinea Connector:

Log in to the Delinea Connector server.

To update the Delinea Connector:

Active Directory Connector

Open the Windows Start menu and start the Delinea Connector Configuration program.



Supported AD Group Types on the Delinea Platform

The Delinea Platform supports the following types of Active Directory (AD) groups for access control:

- Global AD Security Groups
- Universal AD Security Groups

These group types are designed to manage and enforce access control effectively, leveraging their compatibility with access control systems such as the Delinea Platform.

Why Distribution Lists Are Not Supported

The Delinea Platform does not support **distribution lists** for access control. While distribution lists, sometimes referred to as "distribution groups," are useful for communication purposes (for example, sending emails to a specified set of users), they are fundamentally unsuitable for managing access permissions.

Purpose of Distribution Lists:

- A distribution list is a mechanism for sending emails to a defined group of recipients. It is optimized for messaging and not for permission management.

Limitations in Access Control:

- Distribution lists cannot be included in Discretionary Access Control Lists (DACLS), which are essential for determining access permissions in systems like the Delinea Platform.
- Unlike security groups, distribution lists do not have an index that can be queried to confirm whether a specific user is a member of the list.
- This lack of searchability makes it impossible to verify if a user attempting to access a resource is part of a distribution list, rendering them ineffective for access control purposes.

Difference Between Security Groups and Distribution Lists:

- **Security Groups:** Used explicitly for access control and can be referenced in DACLs to enforce permissions.
- **Distribution Lists:** Only serve as a tool for communication and are not designed to interact with access control mechanisms.

Using Connector Best Practices

When using the Delinea Connector, keep the following best practices in mind.

Supporting User Authentication for Multiple Domains



Note: If all your Delinea Platform users have their accounts on a single domain controller, you can skip this topic.

You install the Delinea Connector on a machine that is joined to Active Directory (AD) to authenticate Delinea Platform users who have accounts in that domain. If you want the Delinea Platform to authenticate users in other domains, you can configure the connector to do so. The technique you use depends on whether the accounts are in trusted domains within a single forest or in multiple forests without trust.

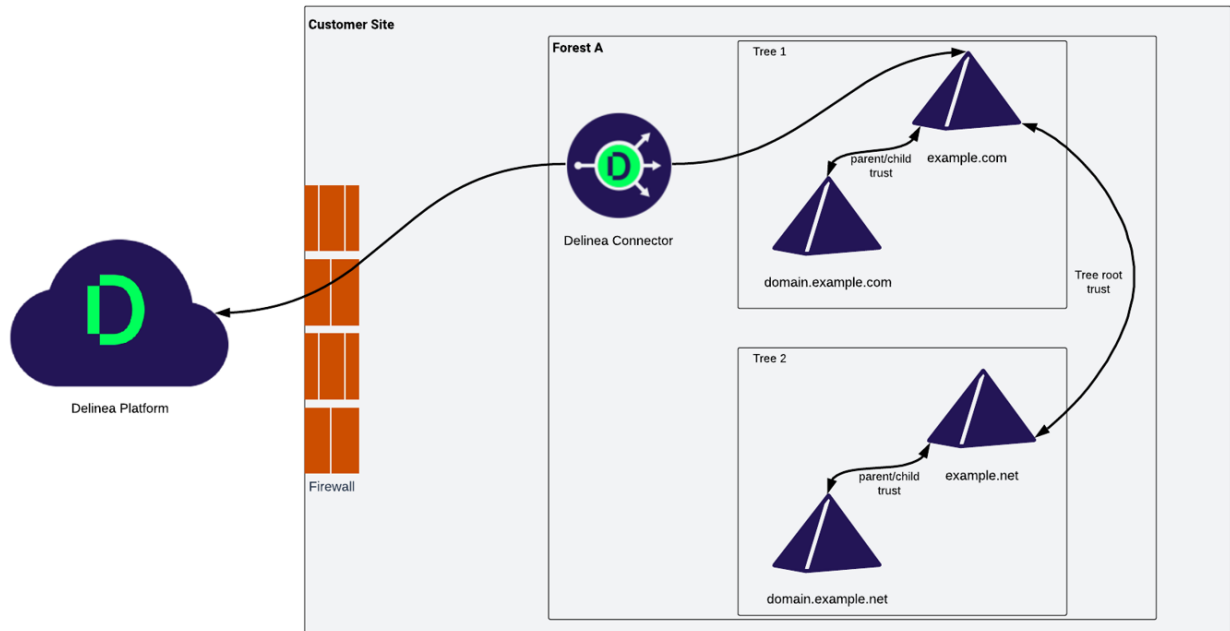
Configuring Authentication for Trusted Domains

Use this technique when users' Active Directory accounts are in one or more domains that have a two-way, transitive trust relationship with the domain the connector is joined to.

In this case, you have a single connector for the entire domain tree within a single forest. After installing the first connector, it is advisable to install one or more on a separate server(s) for additional resiliency. The host server for each connector must be joined to the same Active Directory domain. For additional details, see "[Installing Additional Delinea Connectors](#)" on page 286.

The platform communicates through this connector for all authentication requests. If the user account is in another domain, authentication requests are handled based on the trust relationships between the domains, such as tree-root, parent-child, forest, and shortcut trust settings.


Trusted Domain Model




By default, two-way transitive trusts are automatically created when a new domain is added to a domain tree or forest root domain using the Active Directory Installation Wizard. The two default trust types are parent-child trusts and tree-root trusts. When configuring the trust relationship, be sure to select Forest Trust. This establishes a transitive trust between one forest root domain and another forest root domain. For more information about trust relationships, see [How Domain and Forest Trusts Work](#) in Microsoft TechNet.

The Delinea Platform automatically creates a login suffix for the domain to which the host computer is joined, plus all the domains that the connector can see. The visibility of domains depends on two criteria:

- **The trust relationship between domains.** All domain trusts in an AD forest with two-way transitive trust meet this criterion.
- **The connector's user account permissions.** By default, the connector is installed as a Local System user account on the Windows host. The permissions granted to this account can affect its ability to see other domains. For more information, see ["Alternate Accounts and Organizational Units Permissions"](#) on page 273.

 **Note:** When the Admin searches Active Directory domains for users and groups (for example, when adding a user or group to a role) in the Delinea Platform, it only searches the Active Directory Users container in the domain controllers visible to the connector.

 **Important:** By default, the connector does not perform cross forest user look-up from a local forest. To enable this functionality, contact the Delinea Support team. Once enabled, avoid installing connectors in each of the forests where trust exists. For example, if you decide to run connectors on machines linked to both Forest A and Forest B, the same user will appear in both forests as distinct users with conflicting IDs and UPNs. This causes considerable confusion among users, because they are seen as separate entities within each forest. This makes the resolution of such issues challenging.

Trusted Domain Model Across Multiple Forest with Trust

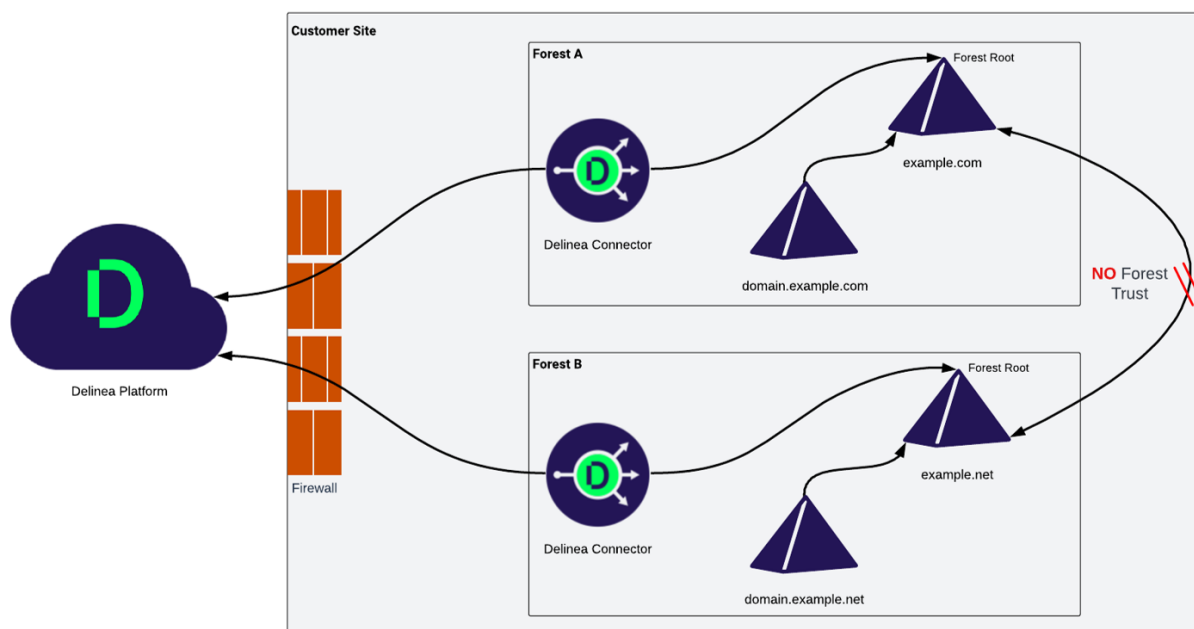
Delinea Delinea Platform

Configuring Authentication for Multiple Forests without Trust

Use this technique when users' Active Directory accounts are in multiple forests without trust, such as in a [restricted access forest model](#) or when you have distinct forests due to organization or administrative boundaries (such as mergers or separate business units).

In this model, a separate connector is designated for each independent domain tree or forest. The Delinea Platform determines which connector to use for the authentication request based on the login-suffix-to-domain mapping it creates and maintains. When a user account resides within the domain controller associated with a connector, the authentication requests are processed according to the tree-root, parent-child, forest, and shortcut trust relationship settings among the domain controllers within that forest or domain tree.

**Multiple Forest Model
Without Trust**



After installing the first connector for each independent domain tree or forest, it is recommended to install one or more additional connectors on separate servers for each domain tree or forest. Each server hosting a connector must be joined to the same Active Directory domain as the initial connector for that specific tree or forest. For detailed instructions, see ["Installing Additional Delinea Connectors"](#) on the next page.

The Delinea Platform automatically generates a login suffix for the domain to which the host computer is joined, as well as for all the domains that are visible to the connectors for each independent domain.

When conducting a search in the Delinea Platform for Active Directory domains for users and groups (for example, when adding a user or group to a role), the search is limited to the Active Directory Users container in the domain controllers accessible by the connectors.

By default, the connector is installed as a Local System user account on the Windows host. The permissions you grant to this account can affect its ability to see other domains. For more information, see ["Alternate Accounts and Organizational Units Permissions"](#) on page 273.

Delinea Connector Redundancy

To ensure continuous uptime for Delinea Platform services, it is advisable to implement redundant connectors by adhering to the following guidelines:

- Deploy two or more connectors for each forest to ensure redundancy.
- Isolate each connector on its own Active Directory server.
- Whenever possible, install each connector in a separate physical location to mitigate the risk of localized failures affecting all connectors.
- Ensure that each connector has its own Internet connection to avoid a single point of failure in network connectivity.
- The Delinea Platform features load balancing across all connectors that have the same services installed. When a request is received, the Delinea Platform distributes the request among the available connectors. Should one connector become unavailable, the platform automatically reroutes the request to the remaining available connectors, ensuring automatic failover.

Installing Additional Delinea Connectors

Use the same procedure to download the installation wizard to the host server, then run the wizard to install and register additional connectors. After you install and register the connector, it is added to the Delinea Connector settings page.

See "Downloading the Delinea Connector and Getting a Registration Code" on page 275 for more information.

Additional Information

- AD changes are pushed from the connector to the platform according to a schedule. You can configure how frequently Active Directory updates, such as user account information or new domain controllers (DCs), are synchronized to the platform by updating the "Setting update interval" configuration field in the Delinea Connector configuration application. The default synchronization interval is 10 minutes. Additional delays may occur as information is fully synchronized, processed, and reflected in the platform. You can force changes to AD users to be picked up earlier by using the 'reload rights' action for a user.
- The connector supports look-up for global AD security groups, universal AD security groups, and user attributes/claims named **groups**. It does **not** support distribution lists. See the **Note** below.
- To automate the installation process of the Delinea Connector, see the [Delinea GitHub repository](#). It contains details on installing the connector through the command line and provides an example script for automating the entire installation procedure.
- Avoid installing the connector on an Active Directory Domain Controller.
- If you are using both the Delinea Connector and federation, the User Mapping settings in the federation configuration should be set to **Required**. This will prevent the creation of duplicate users by disabling the ability to create local users when mapping is not possible. For more information, see [Mapping Federated Users](#).



Note: The platform supports the following types of groups: global AD security groups, universal AD security groups, Entra ID security groups, and user attributes/claims named **groups**.

It does not support domain local groups. It also does not support distribution lists. A **distribution list**, sometimes inaccurately called a *distribution group*, is used to send email to users specified on the list. But on any access control system including the Delinea Platform, groups are used for access control. A distribution list cannot be used for access control because it cannot be listed in discretionary access control lists (DACLS). A distribution list has no index, so you can't query it to determine if a user (trying to access something) is or is not on the list, rendering the distribution list useless for purposes of controlling access.

Troubleshooting the Delinea Connector

This page tells how to investigate and solve issues related to the Delinea Connector.

Platform Can't Map a Federated User to an AD User

Check that all claims are correct. If all claims are correct, try re-registering the Delinea Connector.

Can't Add Local User with Duplicate Login ID

Given that a domain-joined user is set up in the Delinea Platform, when trying to later add a local user with the same User Principle Name (UPN), it cannot be added, even if the domain-joined user is deleted. An error message like the following occurs:

User name name@domain.com is already in use

When creating a local user in the platform, the platform will try to avoid creating duplicate objects by checking all available directories for the UPN before creating the user.

Remove the Connector to add the local user. To re-enable secure communication between the Delinea Platform and AD directories, reinstall the Connector. Also see [Troubleshooting Federated Group Mapping](#).

Invalid Certificate Error Installing Connector

The remote certificate is invalid according to the validation procedure.

Resolution: This issue is commonly triggered by active deep SSL inspection, which must be disabled. Ensure that the IP addresses specified under "Platform Architecture" on page 79 are allowed.

Missing or Unverified Certificate Error Installing Connector

Failed to obtain certificate or certificate verification failed.

Resolution:

1. Make sure your Windows updates are up to date.
2. Verify the accessibility of Certificate Revocation Lists (CRLs) by confirming access to the following:
 - <http://cps.letsencrypt.org>
 - <http://r11.o.lencr.org/>

- `http://x1.c.lencr.org/` (the CRL endpoint for the issuing subordinate CA, required to allow successful TLS negotiation and certificate chain check)

Unhandled Exception Error Installing Connector

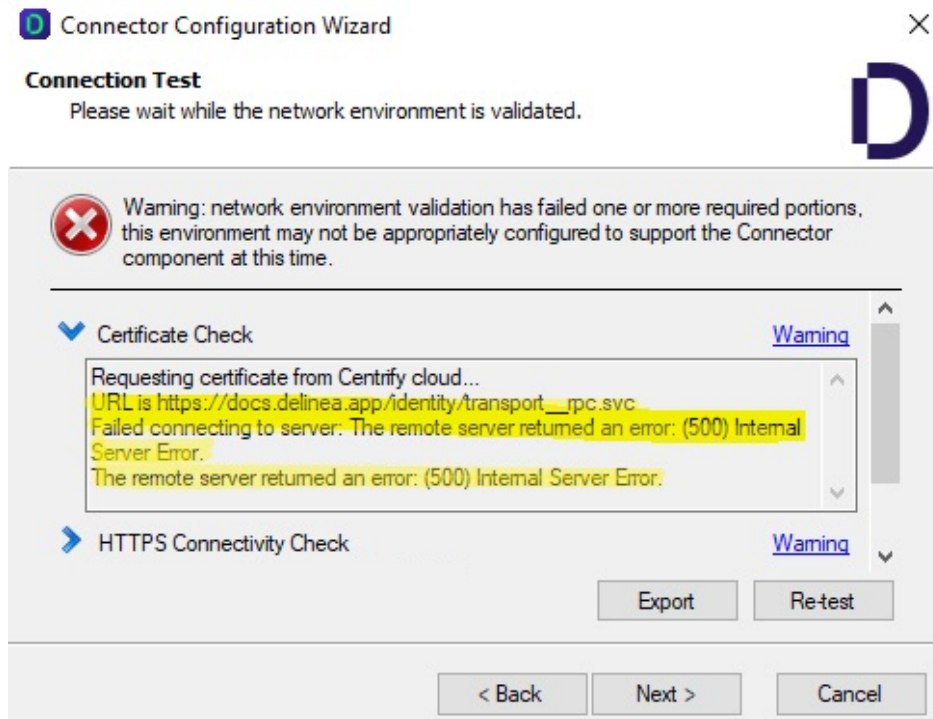
Encountered unhandled exception in registering the proxy:

System.ServiceModel.EndpointNotFoundException: There was no endpoint listening at `http://<tenant url>/transport_rpc.svc`

Resolution: Ensure that you are running the latest version of the Connector and try again.

Certificate Check Error Registering Connector

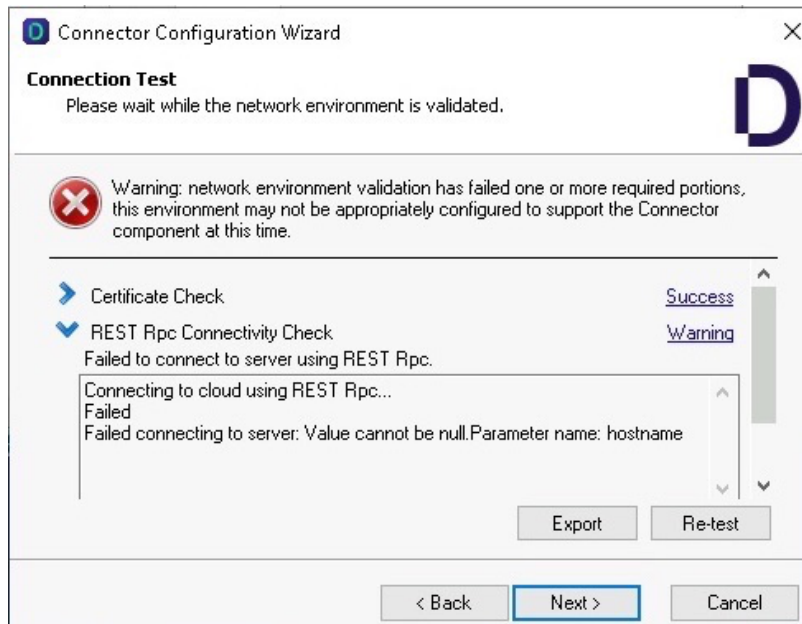
(500) Internal Server Error



Ensure that you are running the latest version of the Connector and try again.

Failed to Connect Error Registering Connector

Failed to connect to server using REST RPC



This error may indicate an incorrect platform tenant URL entry. Please revisit the platform tenant URL you provided and ensure its accuracy before attempting to register again.

Delinea Connector Configuration Application Stalls

This lasts for several minutes and the application is not accessible.

Check to see if any endpoint security applications such as SentinelOne are active on the host where the Connector is located, as they might disrupt the Connector during installation or registration.

Connector Fails to Connect to Platform

All connections from the Connector to the platform are outbound. No internet-facing ingress ports are required for the Connector. For more information, refer to "[Platform Architecture](#)" on page 79. If you use a proxy with the Connector, ensure that connectivity is established and that name resolution functions correctly. Search within your environment for potential issues originating from firewalls or packet inspection solutions, particularly those that could affect communication between the Connector and the platform.

Delinea Connector Auto-update not Working

AutoUpdate support was added after 4.1.x versions. Manually upgrade to the latest version of the Connector to take advantage of auto-update.

Authentication Fails After Connector Installed and Active

They get this error message: ***Authentication (login or challenge) has failed. Please try again or contact your system administrator.***

Privileged Remote Access

- Verify that the user is entering accurate Active Directory credentials to log in to the platform.
- Examine the Delinea Connector logs for potential errors.
- Investigate whether the issue is isolated to a particular user, and assess any unique factors (e.g., expired account).
- Confirm that the Connector status is active.
- Check connectivity using a Ping operation from the platform to the Connector.

Where Can I Access the Delinea Connector Logs?

Connector logs (such as log.txt) can be reviewed under C:\Program Files\Delinea\Delinea Connector

What are the Default Rotation Settings for Connector Logs?

The default maximum log file size is 2 MB, and the default maximum number of log backup entries is 450.

What are Best Practices for using Federation and Active Directory Together?

1. First set up the Connector so that on-premise AD is visible to your platform tenant.
2. Then set up federation with mapping of users enabled as optional. This will cause federated users to become (map to) the AD users if possible when they log into the tenant.

Can't Query Active Directory Users or Groups After Connector Installed and Active

Upon inspection, I see a warning on the Connector configuration screen stating, "This Connector may not be discoverable from other computers," and there's an error in the logs saying, "Failed to create or get proxy SCP."

This could indicate a communication problem between the machine running the Connector and the Active Directory Domain Controller. Follow these steps to address this issue:

1. Remove the machine object (that has the Connector) in Active Directory.
2. Re-join the machine to the domain.
3. Re-install the connector.

Privileged Remote Access

Delinea Privileged Remote Access (PRA) provides seamless access to remote machines through RDP (Remote Desktop Protocol) and SSH (Secure Socket Shell) without the need for a VPN (Virtual Private Network).

Delinea PRA runs on the Delinea Platform and seamlessly integrates with Delinea Secret Server vault, deployed from the cloud or from within a customer's private network. PRA automatically uses credentials to connect with target resources, enabling RDP and SSH connectivity as well as SMB and SFTP file transfers without exposing sensitive parts of credentials to the end user. This fast and simple workflow is completely integrated into the Delinea Platform user interface.


Delinea PRA displays RDP and SSH sessions in the user's web browser, enabling the user to access multiple connections to multiple target systems, each running in its own tab in the user's browser.

When a user requests a connection to a remote target, they connect to the Delinea Platform first with their browser. If authorized, the Delinea PRA workload facilitates the connection with the target machine. The PRA workload is also used to integrate Secret Server On Premise installations with the Delinea Platform.

For additional security, PRA sessions can be configured to be observed in close-to-real time and can be recorded for auditing purposes.

The PRA workload works for both Windows and Linux.


Setting Up the PRA Engine

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

The content in this section is intended for tenant administrators of the Delinea Platform managing PRA sites and engines. It provides the [requirements](#) for setting up PRA on the platform, instructions on how to [add secret templates](#) to PRA, how to set up a [PRA engines site](#), and how to [install](#), [activate](#), and [uninstall](#) PRA engines.

Other sections provide instructions for PRA [user tasks](#), and for PRA session recording.


PRA Requirements

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

Delinea PRA runs in the Delinea cloud and connects to target servers using the Delinea PRA Engine, which has a small footprint and runs on a variety of Linux distributions.

■ Supported Operating Systems:


- Amazon Linux 2
- Amazon Linux 2023+
- Debian 8+
- Red Hat EL 8+
- Ubuntu 18.X+


 **Note:** PRA only supports operating systems that have not reached their official End-of-Life date. For best performance and compatibility, we highly recommend deploying PRA engines on actively supported versions of the operating systems specified above.

- **CPU:** x86-64 based processors at 2.5 GHz or higher, 2 or more cores are recommended for production use
- **Memory:** 32 GB recommended for production usage

Privileged Remote Access

- **Storage:** 100 MB or more recommended for installation and runtime needs
- **Firewall Rules:** 443 TCP Outbound Open
- **Network:** The PRA engine will function as long as the remote target server or Secret Server On Premises can be found via an IP address or DNS look-up and is reachable on the Local Area Network or via routing tables.
- **Supported Web Browsers and Limitations:** See list of [Supported Browsers](#) and limitations.

 **Important:** You may be able to install the engine software on host servers that do not meet these parameters, including other Linux downstream or independent distributions and versions. However, these installations are not supported by Delinea and would be made at your own risk


 **Note:** To learn more about using Privileged Remote Access with Secret Server on-premise, please refer to ["Connecting to Secret Server On Premise"](#) on page 796

Useful Tools

The following tools are not necessary to run a PRA engine, but may be useful with troubleshooting if needed:

- netstat
- journalctl
- telnet
- netcat
- df
- top
- free
- vmstat

Sizing for PRA Engine Linux Hosts

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see ["Upgrading Standalone PRA Engine to the Delinea Platform Engine"](#) on page 309

The PRA engine runs on supported Linux hosts (for more information, see ["PRA Requirements"](#) on the [previous page](#)) and is used to establish connections between a user's browser and target systems within the customer's private network. When a connection is initiated, the PRA service in the Delinea Platform selects a single PRA engine from a set of engines associated with the parent site, to host the connection.

This document offers guidance to users to determine what hardware configuration is needed to host the PRA engine depending on the number of concurrent PRA session that engine needs to host.

Size testing was performed on PRA engine hosts running Ubuntu version 18.04.3 LTS equipped with 4 Intel® Xeon® E5-2609v3 CPU cores @ 1.9 GHz, with 8GB of RAM, on a 10mbps network.

Sessions were tested on a site with a single PRA engine, as well as a site associated with two PRA engines. Multiple concurrent sessions were opened, kept running for 30 minutes and then closed. The following actions were performed on the remote target machines after connection was established:

Privileged Remote Access

1. SSH: Login to a remote Linux server and run “top”.
2. RDP: Login to a remote Windows server and run a batch script that produces output similar to that of a typical command-shell script.

Session recording was disabled in both test cases.

Session Type	# of PRA Engines	# of Concurrent Sessions	% Per-engine CPU usage	% Per-engine Memory usage
SSH	1	200	8	40
SSH	2	400	8	38
RDP	1	200	19	40
RDP	2	400	17	41

While a Single PRA engine can handle 200 SSH or RDP sessions concurrently, your actual capacity may vary depending on the specific activities that are being carried out on the remote target machine. For example, viewing a video clip on the remote machine on RDP will put very different load on PRA as compared to running vim to edit a text file on a remote SSH session. Performance test data also indicates that PRA engine performance is more dependent on memory and bandwidth than CPU speed or power.

The network latency between the end-user’s browser and the Delinea Platform, or the latency between the PRA engine and the target server also affects the user-experience.

We recommend the following steps when experiencing PRA performance issues that may be associated with PRA engines:

1. Use system monitoring tools to determine whether any specific resource like memory, network bandwidth, CPU utilization is running at unacceptably high levels. If possible, increase the corresponding hardware or virtualization resources.
2. Deploy more engines to the parent site.
3. Check the network latency between:
 - a. The PRA engine and the Delinea Platform tenant.
 - b. The PRA engine and target machines
4. Contact Delinea Support.

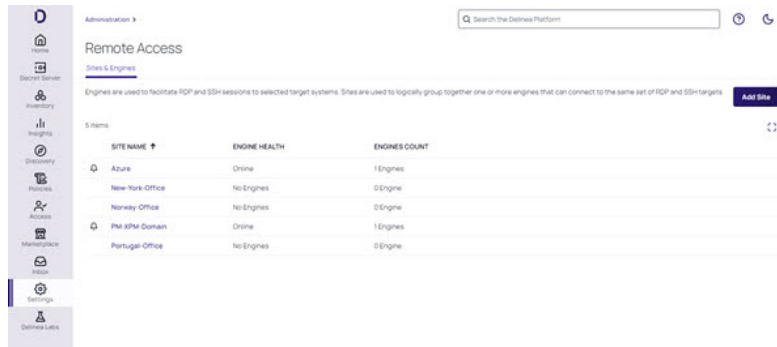
Setting Up a PRA Engines Site



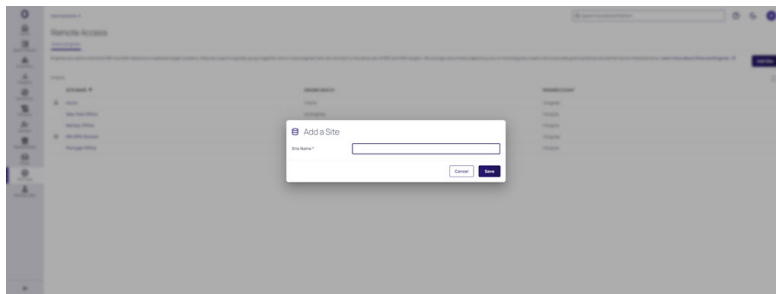
Important: This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

Privileged Remote Access

1. SSH into the on-premises server where you would like to install the PRA engine, and log in with administrative privileges.
2. From the left navigation menu, click **Settings**, then click **Remote access**. The **Sites & Engines** tab appears.
3. On the **Sites & Engines** tab, Click the **+Add Site** button.



4. On the **Add a Site** page, enter a descriptive site name; for example, secret-server. You can use only letters, number, hyphens, and underscores in the name.

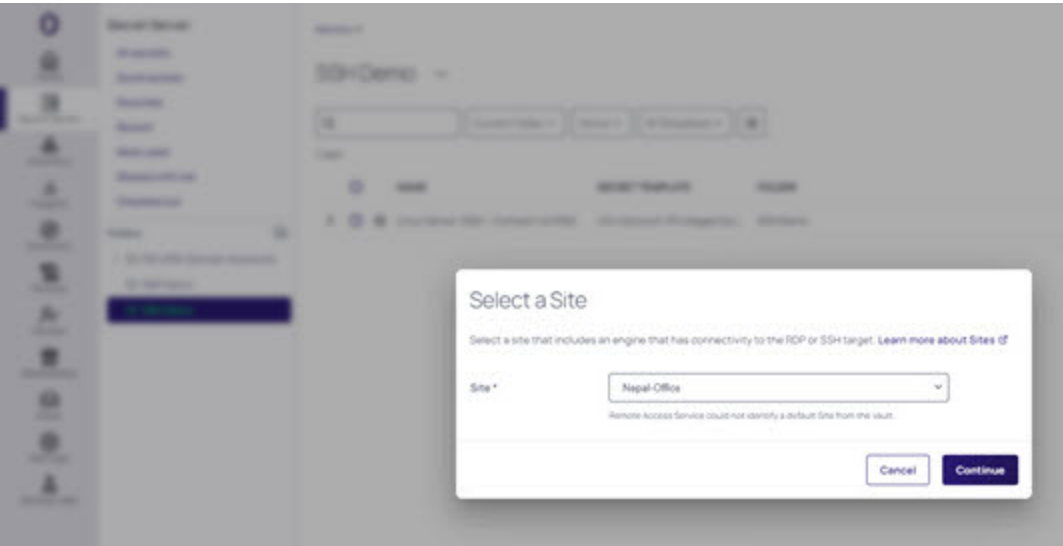
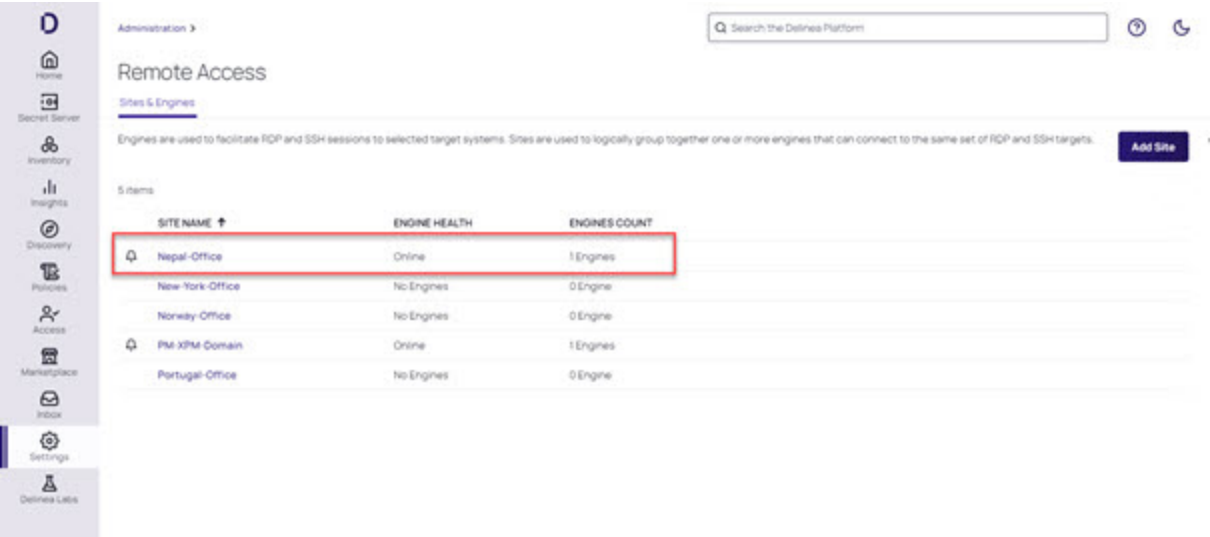


5. Click **Save**.

Naming a PRA Site

Delinea recommends that tenants use the same name for both PRA Engine sites and secret sites. This way, when a user selects a secret, the preferred PRA Engine site is automatically pre-selected when launching that session. Without this practice, users would have to manually select a PRA site, and might select the wrong one.

Privileged Remote Access



Renaming PRA Site

1. From the left navigation menu, click **Settings**, then click **Remote access**.
2. Click the **More Actions** menu next to the site name.

Privileged Remote Access

Settings

Overview

Connection points

Sites and engines

Connectors

Registration codes

Remote access

Directory integrations

Federation providers

Directory services

User attributes

MFA and security

Authentication profiles

MFA providers

Security questions

Security devices

Global security

Corporate IP range

Secret Server

Administration

Secret Server connection

Platform groups sync

Tenant customization

Behavioral Analytics

Platform Setup

Administration >

Remote Access

Sites & Engines

Engines are used to facilitate RDP and SSH sessions to selected target systems. Sites are used to logically group together one or more engines that can connect to the same set of RDP and SSH targets. We strongly recommend deploying two or more engines in each site to provide good resilience and performance characteristics. Learn more about Sites and Engines. [Add Site](#)

4 items

SITE NAME ↑	ENGINE HEALTH	ENGINES COUNT
Negal-Office	Online	1 Engines
New-York-Office	More actions 0 Engines	0 Engines
PM-XPIM-Domain	Online	1 Engines
Portugal-Office	No Engines	0 Engines

3. Click **Edit Name**.

Settings

Overview

Connection points

Sites and engines

Connectors

Registration codes

Remote access

Directory integrations

Federation providers

Directory services

User attributes

MFA and security

Authentication profiles

MFA providers

Security questions

Security devices

Global security

Corporate IP range

Secret Server

Administration

Secret Server connection

Platform groups sync

Tenant customization

Behavioral Analytics

Platform Setup

Administration >


Remote Access

Sites & Engines

Engines are used to facilitate RDP and SSH sessions to selected target systems. Sites are used to logically group together one or more engines that can connect to the same set of RDP and SSH targets. We strongly recommend deploying two or more engines in each site to provide good resilience and performance characteristics. Learn more about Sites and Engines. [Add Site](#)

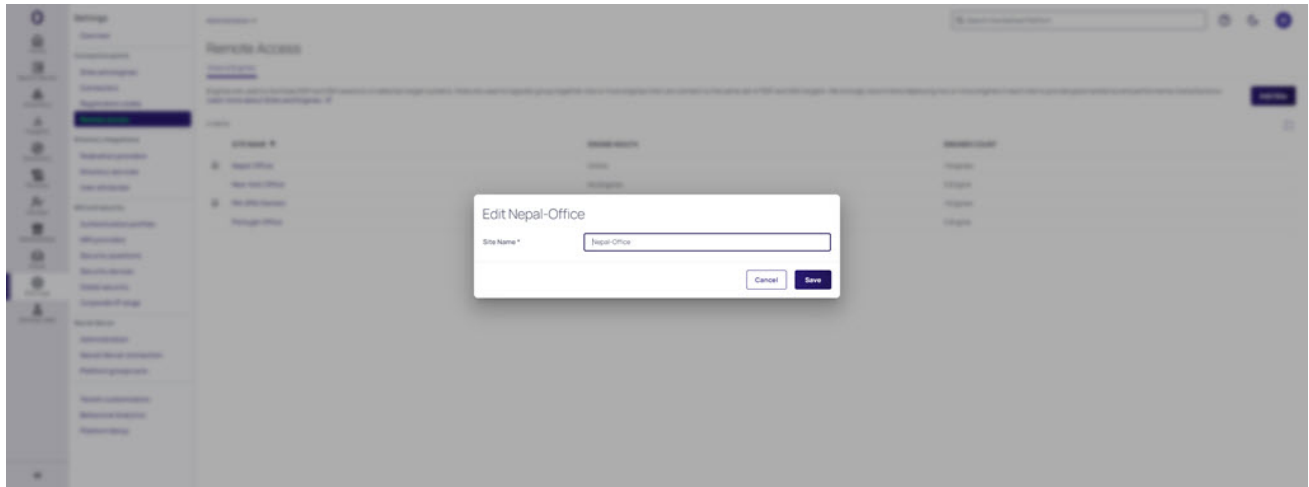
4 items

SITE NAME ↑	ENGINE HEALTH	ENGINES COUNT
Negal-Office	Online	1 Engines
New-York-Office	<div>Delete</div>	0 Engines
PM-XPIM-Domain	<div>Install Engine</div>	1 Engines
Portugal-Office	<div>Edit Name</div>	0 Engines

 **Note:** If you do not see **Edit Name** in the menu, you do not have the needed permissions to edit the name of that particular site.

Privileged Remote Access

5. The *Edit Site Name* dialog box appears.



6. Enter the new name of the PRA site.
7. Click **Save**.

 **Note:** If the save fails, an error message is displayed explaining the cause of the error.

Configuring PRA

In the Configurations tab, you can customize the remote desktop experience for your tenant.

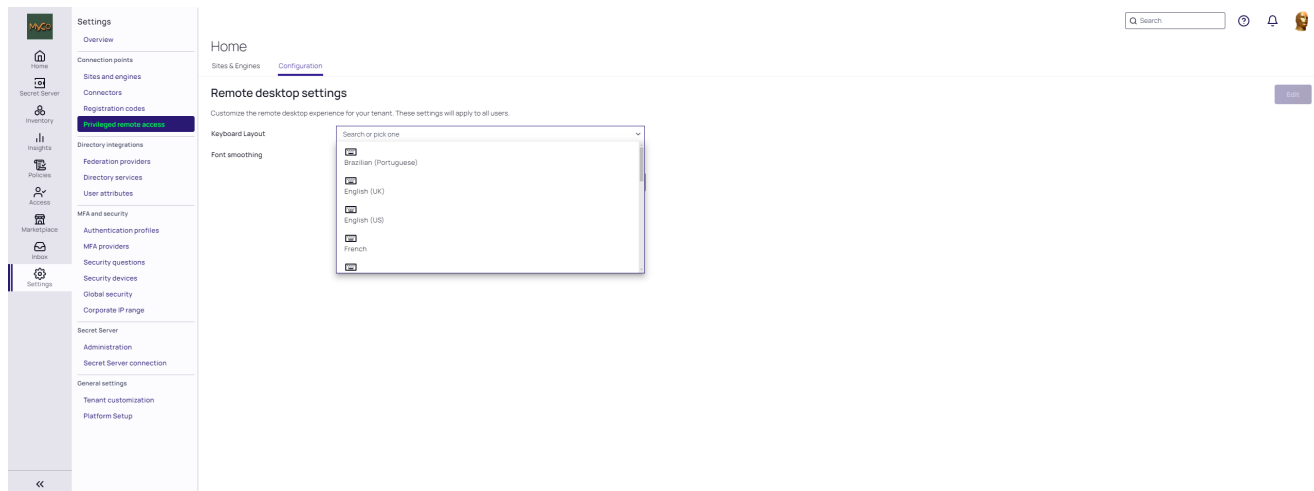
Customize the Keyboard Layout

Keyboard settings for RDP may be needed when the default keyboard is not US English. This setting will apply to all RDP targets by default, but may be overridden for specific remote targets from the Delinea Menu. ([Learn more](#))

To select a keyboard layout:

1. Click **Edit**
2. Select the desired keyboard layout from the dropdown menu.

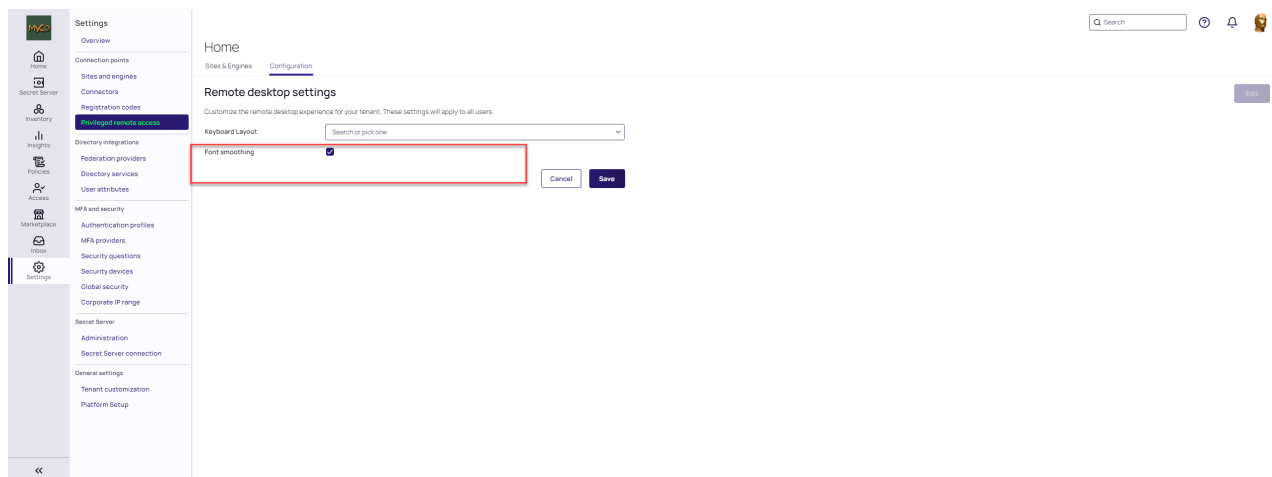
Privileged Remote Access




Font Smoothing

Font smoothing is a technique that can improve the appearance of text on a computer display. When disabled, text over RDP will have jagged edges. Disable this setting if you need to improve performance due to limited network bandwidth. To disable font smoothing:

1. Click **Edit**
2. Check the **Font smoothing** box



 **Note:** ClearType must also be enabled on the remote target machine to support font-smoothing.

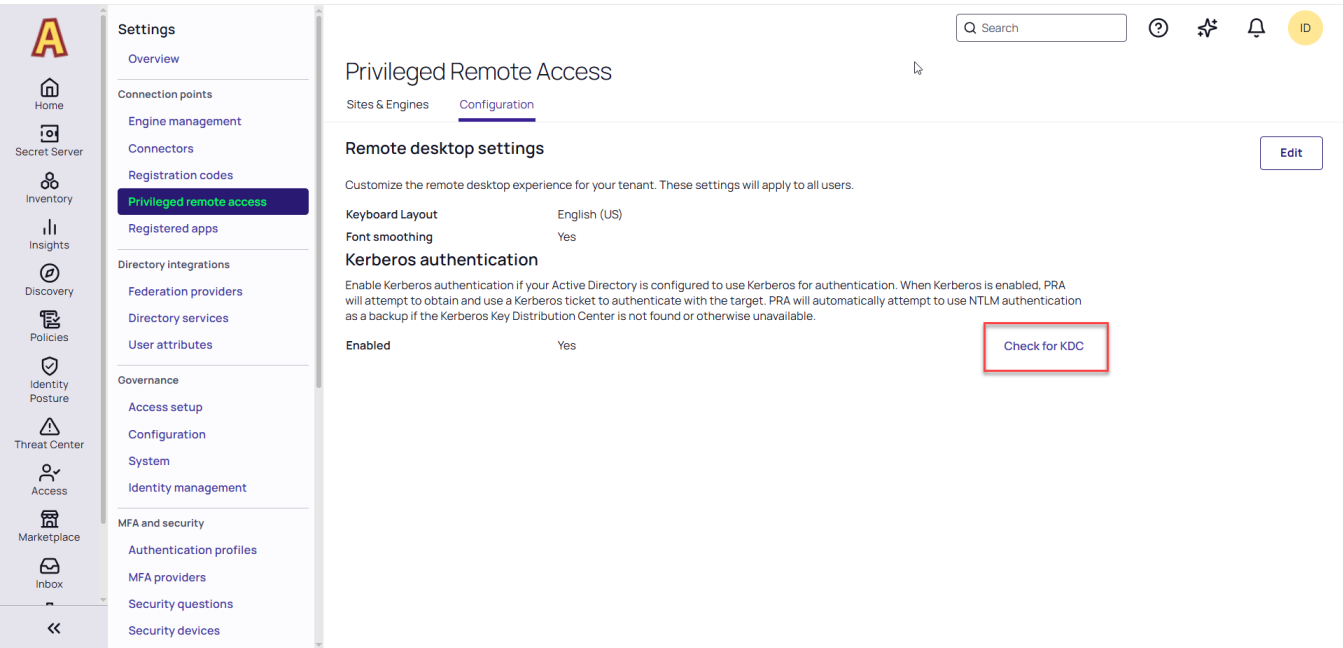
Kerberos Authentication

PRA supports authentication to Windows RDP targets using Kerberos Tickets which is a stronger form of authentication as compared to NTLM. This feature is also required when using Active Directory Protected Users security groups.

Privileged Remote Access

When you select Kerberos authentication, PRA will first try to connect to the Windows target using Kerberos. If authentication with Kerberos fails, PRA will attempt to connect with NTLM.

You can test for Kerberos KDC resolution and connectivity at any time by using the **Check for KDC** button.



Select the name of an existing site with a PRA workload and enter the domain name associated with the KDC and click Test. The test is independent of whether or not Kerberos has been enabled for PRA.

Test KDC connectivity

To verify connectivity to KDC (Key Distribution Center) for Kerberos authentication, select the appropriate Site from the dropdown and enter a Kerberos enabled domain.

Site

Chicago

KDC Hostname or Domain

mycompany.local

Test

Close

Secret Template Requirements

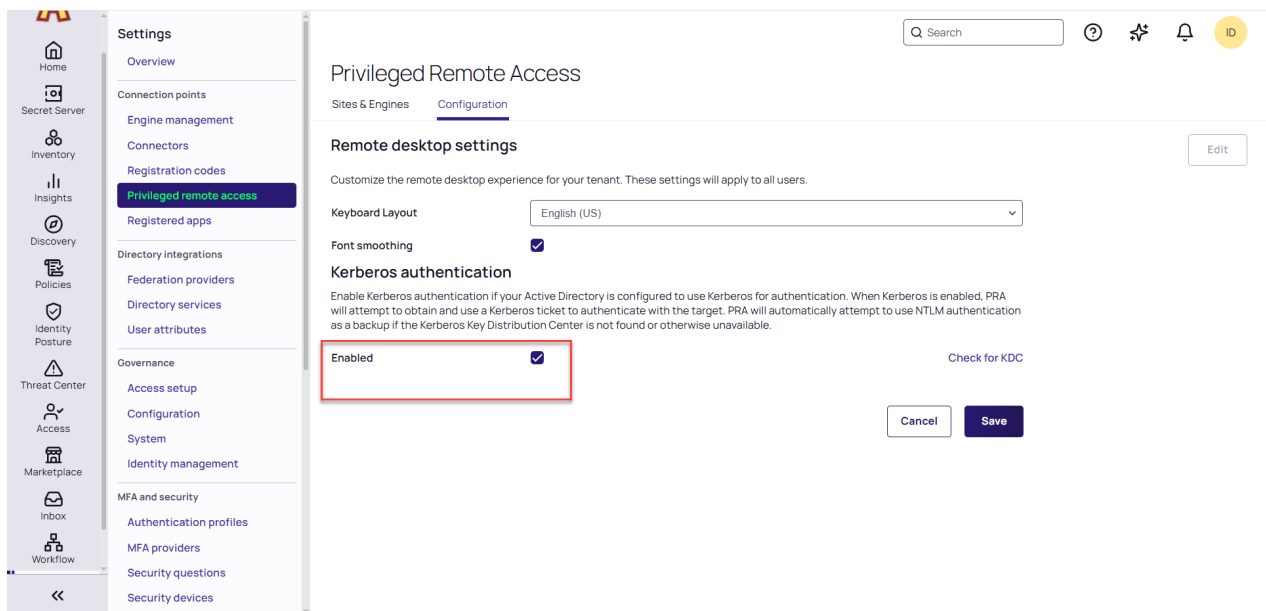
Kerberos authentication also depends on the parameters in the secret templates. Below are the requirements for the Windows Account and Active Directory Account templates:


- For the Windows Account secret template, the Username must be in UPN format. (e.g. artdecco@mycompany.com)
- For the Windows Account template, Machine field (target) in FQDN format (e.g. server01.mycompany.com), Username in UPN format (e.g. artdecco@mycompany.com)
- For Active Directory Account template: Domain and Computer(target) fields in FQDN format (e.g. server01.mycompany.com)

Enabling Kerberos Authentication

To enable Kerberos authentication:


1. On the Privileged Remote Access Settings page, click on the **Configurations** tab.
2. Click **Edit**.
 - a. Check the **Enable** box under *Kerberos authentication*.



 **Note:** When a Secret Server RDP proxy is in use, authentication between the proxy and the PRA engine/workload is done with NTLM, even when Kerberos is enabled with PRA.

You can test for Kerberos KDC resolution and connectivity at any time by using the **Check for KDC** button.


Installing PRA Engines

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

This page gives instructions for installing the PRA Engine.


Engine Rules

- You must first set up a Site before you can install a PRA engine. See [Set Up a PRA Site](#) for options with detailed instructions.
- Only one PRA engine may be installed on any given on-premise PRA server.
- Delinea recommends installing a minimum of two Platform Engines per site with PRA capabilities

 **Note:** This setup will support remote session balancing in order to ensure high availability for remote sessions. PRA efficiently distributes the sessions across workloads on multiple engines, irrespective of the host operating systems.

- Engine names must be unique per site.
- Engine names can contain only letters, numbers, hyphens, and underscores.
- While an engine is in the process of updating, existing PRA sessions will continue uninterrupted. However, new sessions will be unable to launch on the engine until the upgrade is complete.

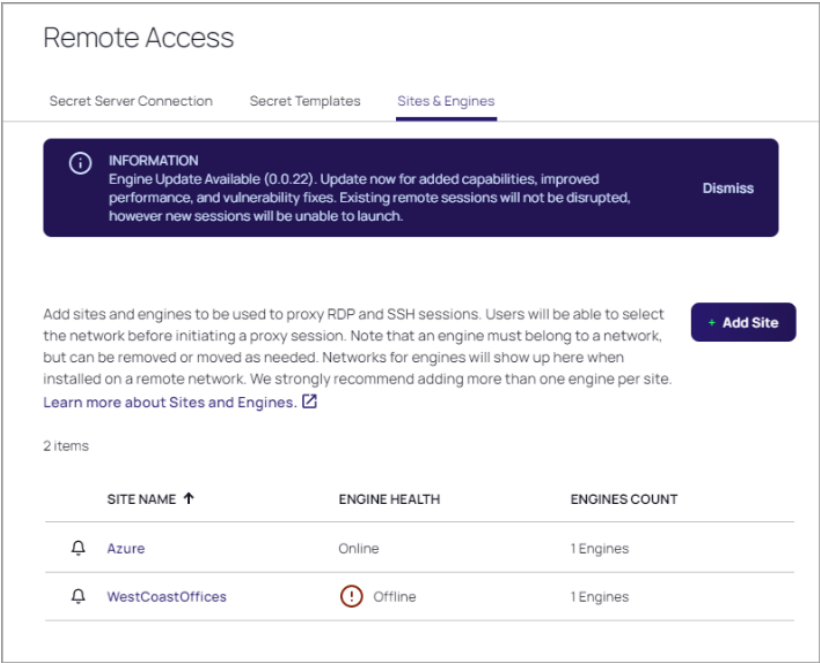
 **Note:** Please review the [PRA Requirements](#) for servers hosting a PRA engine.

 **Important:** The SSH/RDP ports are set in the secret. Please review the [Secret Server documentation](#) for additional information. The PRA engine will use these ports to connect with the downstream targets.

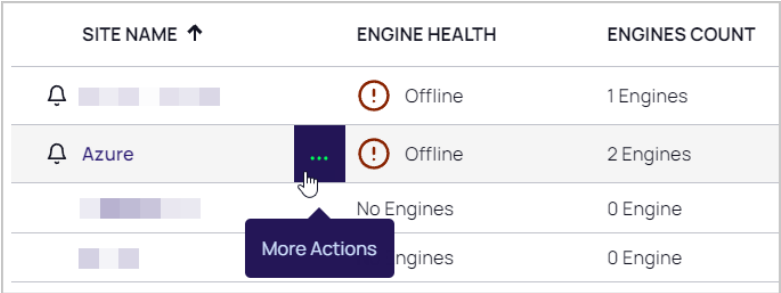
Installing the Remote Access Engine

1. Log in to the platform with administrative privileges.
2. From the left navigation menu, click **Settings**, then click **Remote access**.
3. On the Remote Access page, click the **Sites & Engines** tab.

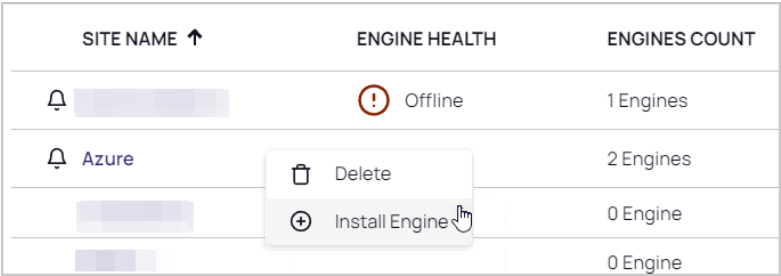
Privileged Remote Access



- 4. Hover your cursor in the site row, at the right side of the **Site Name** column.
- 5. Click the ellipses . . . that appears

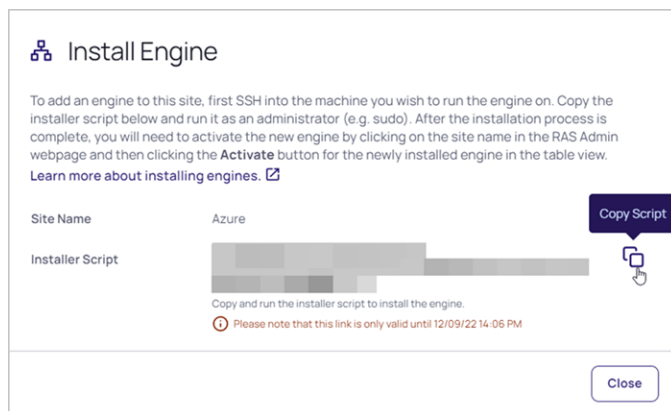


- 6. From the pop-up click **Install Engine**.



- 7. On the **Install Engine** page, you can copy the entire installer script to your system clipboard either of two ways:
 - Select the entire installer script using your cursor and hit `Ctrl-C`.
 - Click the copy icon to the right.

Privileged Remote Access



Installation Script Rules

- If you quit the installation process before it finishes, you will need to start again from the beginning.
- The installer script is for one-time use only, and it expires after ten minutes.

Run the Installation Script

1. SSH into the server you where you would like to install the PRA engine.
2. Log in with administrative privileges.
3. Paste the installer script from your clipboard and run it.
4. Provide your inputs when prompted.
5. When the script completes, a success message will appear.
6. You can validate the installation using the command below, but the software won't be functional until you [activate](#) it through the web interface.

```
[ec2-user@ip-10-200-21-138 ~]$ sudo /opt/delinea/clientmgr -v  
version: v0.0.23, build: 20221024112128
```

Configuring the PRA Engine to Use a Proxy Server (Optional)

You can configure the PRA engine to work with a proxy server by following these steps:

1. Create an environment file by running the following command:

```
sudo vi /opt/delinea/environment
```

2. Add the following line to the file you just created:

```
HTTPS_PROXY=https://proxy.url.here:portHere
```

Privileged Remote Access

3. Save and close the file.
4. You need to add the following `EnvironmentFile` attribute to the `Service` section of the PRA engine systemd unit file:

```
EnvironmentFile=/opt/delinea/environment
```

5. Open the unit file for editing

```
sudo vi /etc/systemd/system/clientmgr.service
```

6. Add the `EnvironmentFile` attribute to the `Service` section

```
[Unit]
Description=On-prem engines client manager.
After=network.target
After=network.target
```

```
[Service]
EnvironmentFile=/opt/delinea/environment
ExecStart=/usr/local/bin/clientmgr
ExecReload=/bin/kill -s HUP $MAINPID
KillMode=process
Restart=on-failure
RestartSec=30
ConfigurationDirectory=clientmgr
StateDirectory=clientmgr
```

```
[Install]
WantedBy=multi-user.target
```

7. Save and close the file.
8. Restart the `clientmgr`


```
sudo systemctl stop clientmgr.service
sudo systemctl daemon-reload
sudo systemctl start clientmgr.service
```

```
[root@rhel7-10-200-21-92 ec2-user]# sudo systemctl stop clientmgr.service
[root@rhel7-10-200-21-92 ec2-user]# sudo systemctl daemon-reload
[root@rhel7-10-200-21-92 ec2-user]# sudo systemctl start clientmgr.service
[root@rhel7-10-200-21-92 ec2-user]#
[root@rhel7-10-200-21-92 ec2-user]# sudo systemctl status clientmgr.service
● clientmgr.service - On-prem engines client manager.
   Loaded: loaded (/opt/delinea/clientmgr.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2023-05-10 17:12:30 UTC; 14s ago
     Main PID: 31159 (clientmgr)
    CGroup: /system.slice/clientmgr.service
            └─31159 /usr/local/bin/clientmgr

May 10 17:12:30 rhel7-10-200-21-92 systemd[1]: Started On-prem engines client manager..
May 10 17:12:30 rhel7-10-200-21-92 clientmgr[31159]: 2023/05/10 17:12:30 version: v0.0.33, build: 20230127100844
```

9. The system administrator may edit the environment file when necessary. After editing this file the system administrator will need to follow the steps above in step 6: *Restart clientmgr*.

Activating PRA Engines

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

- 1. Log into the platform with your administrative account.
- 2. Click **Settings** from the left navigation menu, then click **Remote access**.
- 3. The Remote Access page opens to the **Sites & Engines** tab.
- 4. Click the site name where you wish to activate an engine.

Remote Access

Secret Server Connection

Secret Templates

Sites & Engines

!

INFORMATION




Engine Update Available (0.0.22). Update now for added capabilities, improved performance, and vulnerability fixes. Existing remote sessions will not be disrupted, however new sessions will be unable to launch.

Dismiss

Add sites and engines to be used to proxy RDP and SSH sessions. Users will be able to select the network before initiating a proxy session. Note that an engine must belong to a network, but can be removed or moved as needed. Networks for engines will show up here when installed on a remote network. We strongly recommend adding more than one engine per site. [Learn more about Sites and Engines.](#)

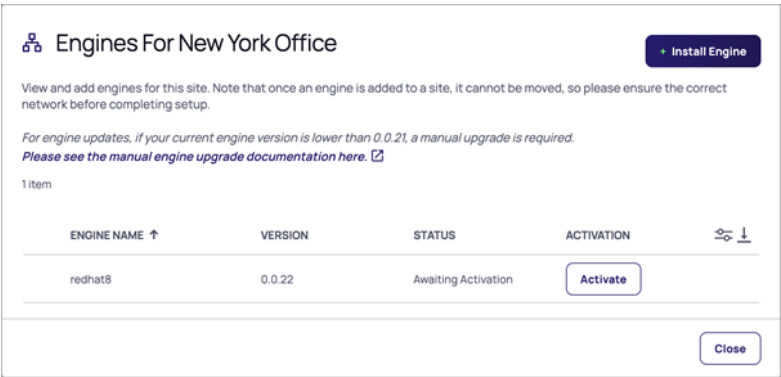
Add Site

2 items

SITE NAME ↑	ENGINE HEALTH	ENGINES COUNT
 Azure	Online	1 Engines
 WestCoastOffices	 Offline	1 Engines

Privileged Remote Access

5. On the Engine page, click **Activate** to bring your new engine online.



Once the engine is activated and the status shows it to be **Online**, you can access and connect to your remote systems through the site and engine.

Adding Secret Templates to PRA

The procedure for adding secret templates to PRA depends on whether you are using Secret Server Cloud or Secret Server On-Premises.

Secret Server Cloud

Secret Server Cloud customers entitled to Privileged Remote Access automatically see the Remote Access launcher link on appropriate launchable secrets. Please refer to the [Secret Server Integration](#) documentation for more information on how to enable Secret Server in your Delinea Platform tenant.

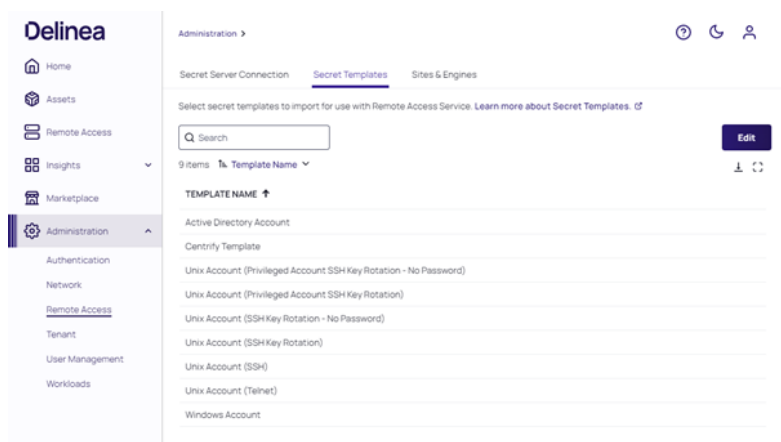
Secret Server On Premises

Before Secret Server On Premises customers can access PRA functionality on the Delinea Platform, administrators must enable one or more secret templates. Only secrets based on PRA -enabled secret templates will be displayed and available to users on the Remote Access page.

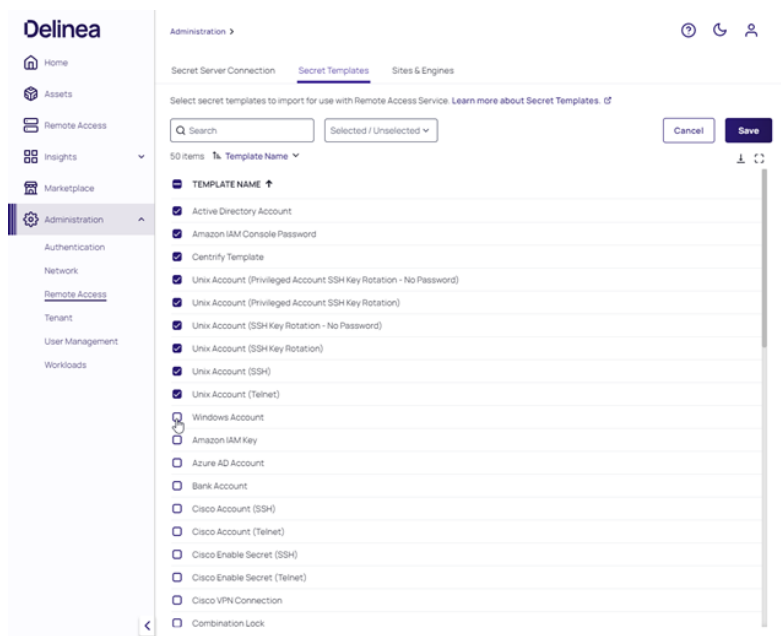
To enable templates for PRA , use the following procedure:

1. From the left navigation menu, click **Settings**, then click **Remote access**.
2. Click the **Secret Templates** tab to display all of the currently available secret templates.

Privileged Remote Access



3. If you would like to add a secret template, click **Edit**.
4. Check the box next to the secret template you would like to add.



5. Click **Save** once you have added all of the needed templates.




Note: The Cloudadmin must be an Admin or at least have View Templates permissions in the on-prem instance.

Uninstalling PRA Engines





Important: This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

Automated Uninstallation


 **Note:** This action removes the PRA engine from the Delinea Platform and completely uninstalls the engine from your host.

1. Log in to Delinea Platform.
2. From the left navigation menu, select **Settings**, then select **Remote access**.
3. Click **Sites & Engines**.
4. Select the site.
5. On the Engine page, find the engine you want to delete and hover your mouse over that row.
6. Click the three dots that appear.
7. Click **Delete**.

ENGINE NAME ↑	VERSION	STATUS	ACTIVATION	
 SeattleOffice	0.0.14	Offline	✓	<div><div>Update</div><div>Delete</div></div>


Close

You should see the following message.

 **Delete Engine?**

You are deleting **redhat8** from **New York Office**

All current remote sessions will be terminated, and engine packages will be deleted from your network.

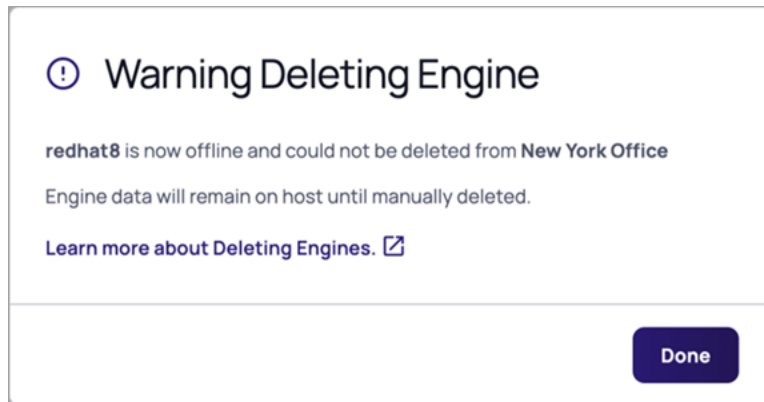
[Learn more about Deleting Engines.](#) 

Cancel

Delete

If the above instructions do not completely uninstall the PRA on-prem engine from your server, you will see the

following warning message:



If you see the warning message above, please follow the steps below to manually uninstall the engine:

Manual Uninstallation

This procedure is for a situation when you absolutely must remove the software from the server and you're unable to do so through the web UI.

If you perform the manual uninstallation procedure, you still need to return to the web UI to delete the engine.

1. SSH into the PRA engine server in question.
2. Run the following CLI command as a privileged user:

```
sudo /opt/delinea/updater -del
```

Upgrading Standalone PRA Engine to the Delinea Platform Engine



Note: This feature is currently available only to customers participating in a Public Preview. For details, see "Public Preview" on page 76

This topic describes how to upgrade a standalone PRA engine to the Delinea Platform engine.

Prerequisites

- The Platform Engine firewall settings introduce additional requirements compared to the existing standalone PRA engines. See "Customer Firewall Requirements" on page 79 for more information.
- Ensure that Linux engine host UUIDs remain the same, even when the host is restarted. See "The Engine Shows as "Offline" " on page 362 for more information.
- Make sure that you have the latest version of the PRA standalone engine installed prior to upgrading. See "Update PRA Engines" on page 319 for more information.



Failure to meet these prerequisites may lead to upgrade failures.

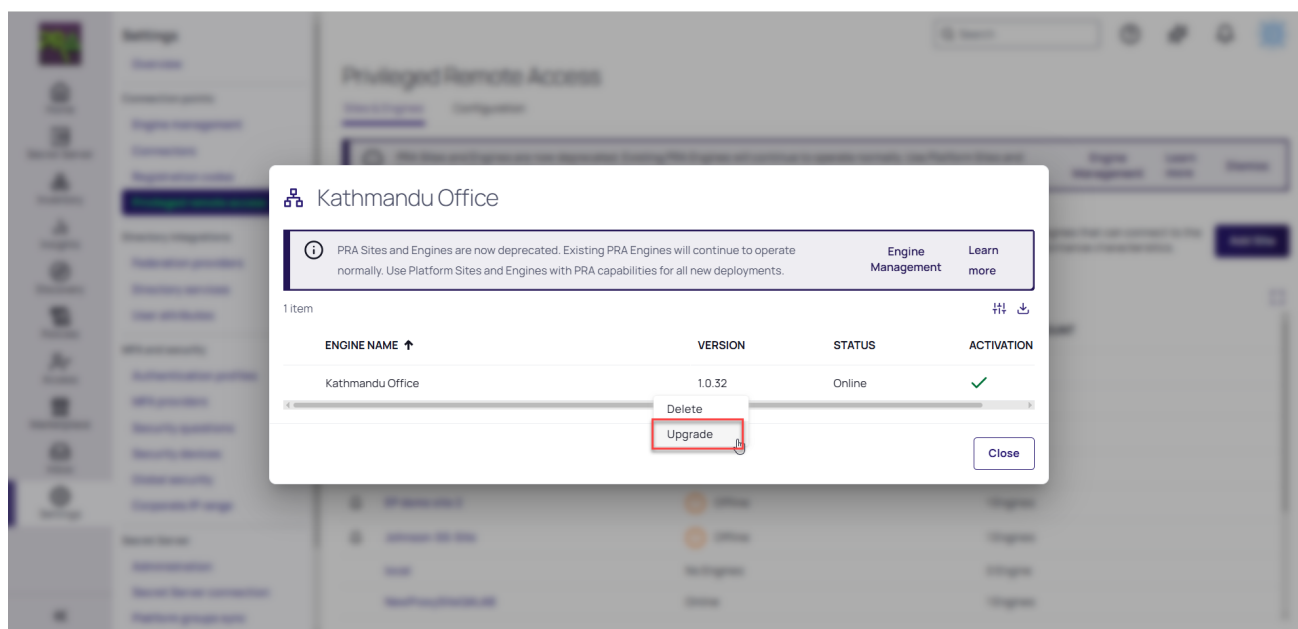
Recommended Best Practices

- **Remove Empty PRA Sites:** It is important to delete legacy PRA sites with no remaining standalone engines. This ensures that PRA uses the correct engines when connecting to remote machines. This step is particularly important after engine upgrades, as engines are moved from *legacy* PRA sites to **Platform sites**.
- **Retain Automatic Site-Selection:** To maintain existing automatic site-selection behavior, customers should create and select Platform sites with the *same name* as the current *legacy* PRA site during engine upgrades.

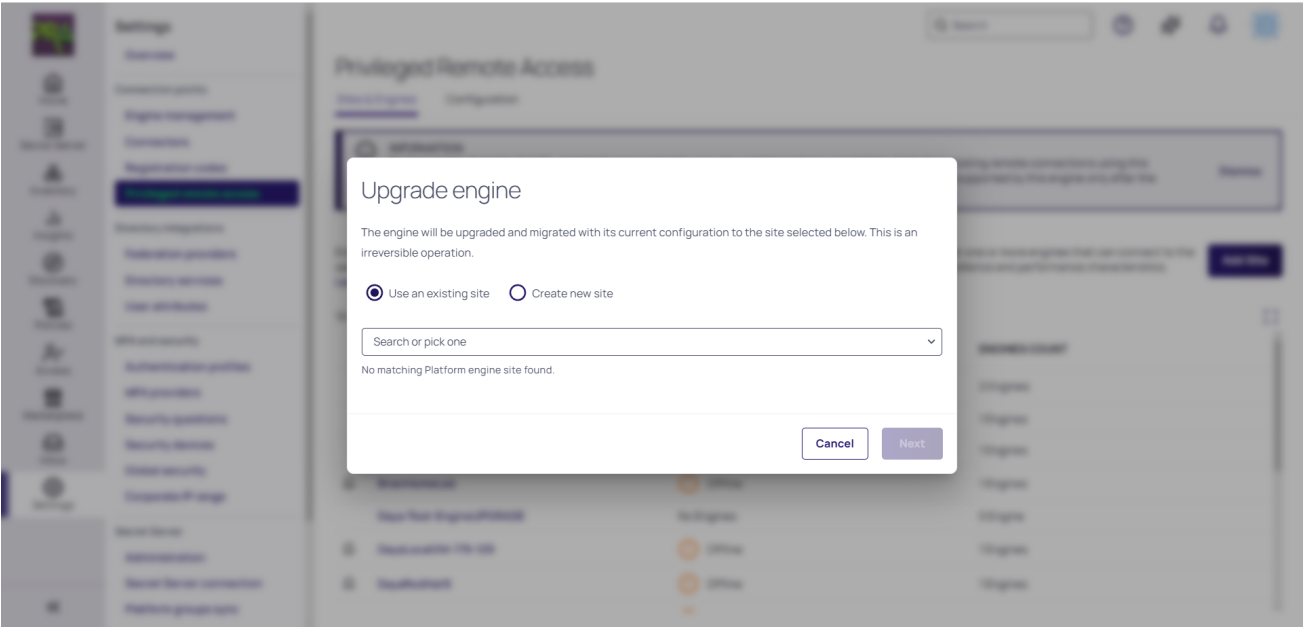
Automatically Upgrading PRA Engines to the Delinea Platform Engine


If you would like to upgrade your legacy PRA engine to the Delinea Engine, follow the steps below:

1. Inside the Delinea Platform, navigate to *Administration > Remote Access*.
2. Click on the *Sites and Engines* tab.
3. Click on a (legacy) site to view all of the engines associated with that site.
4. Find the standalone engine you would like to upgrade and click the three-dot symbol next to the engine.
5. Click **Upgrade**.

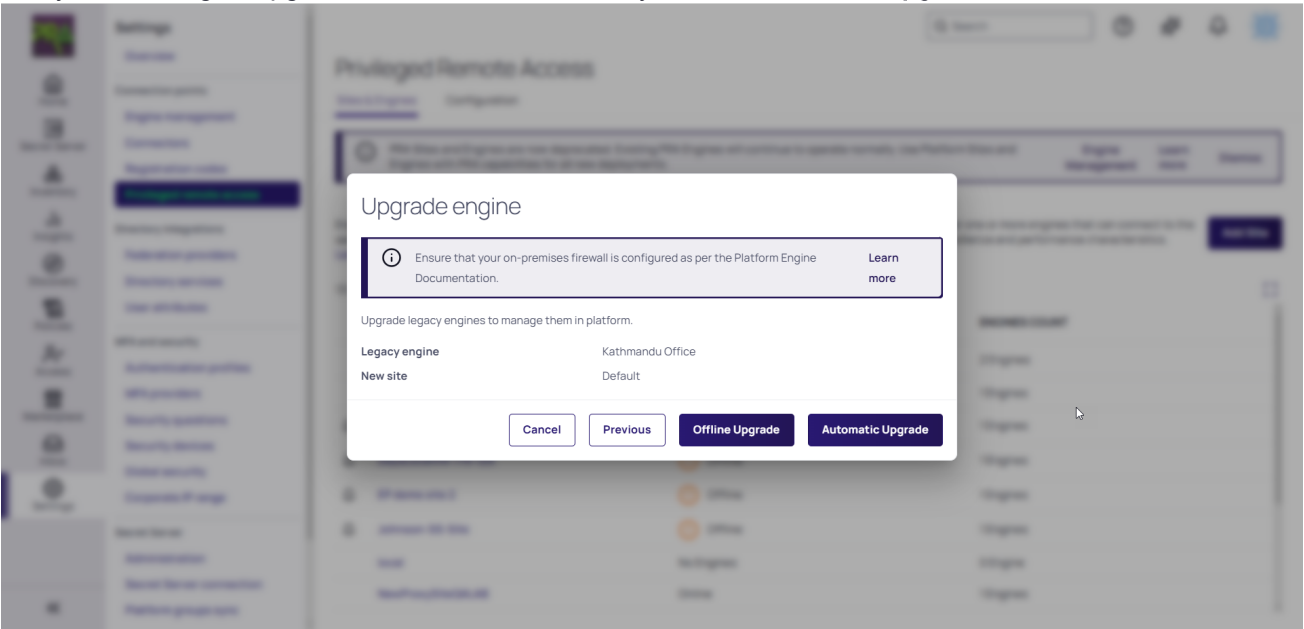


6. Select a [Platform Engine](#) site to include the upgraded engine and click **Next**.

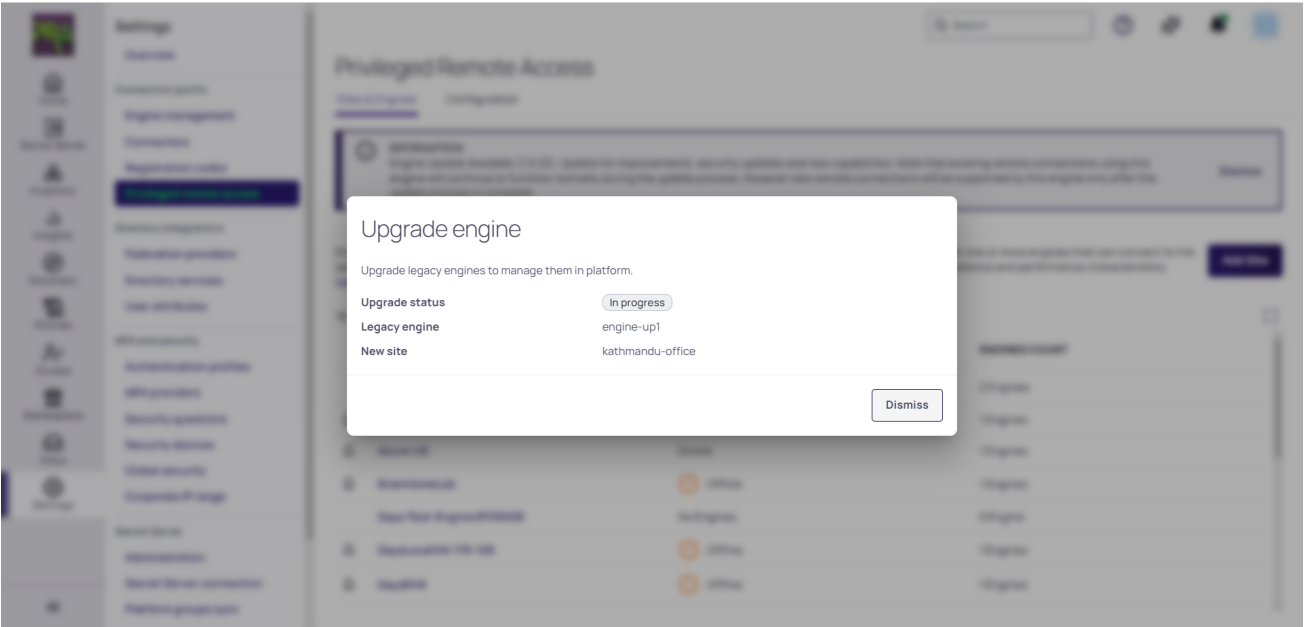


 **Note:** If a Platform engine site with the same name as the deprecated PRA site is found, it will be automatically pre-selected. You also have the option to create a new Platform site.

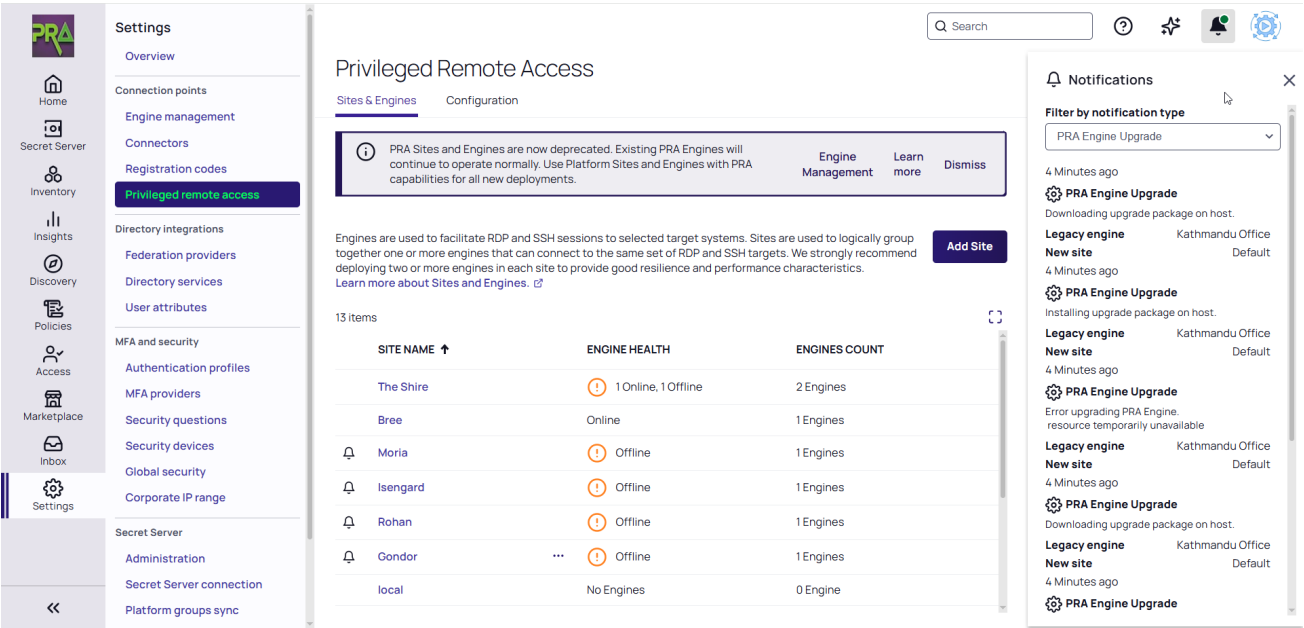
7. Verify that the engine upgrade information is correct. If yes, click **Automatic Upgrade**.



8. The automatic engine upgrade will begin.

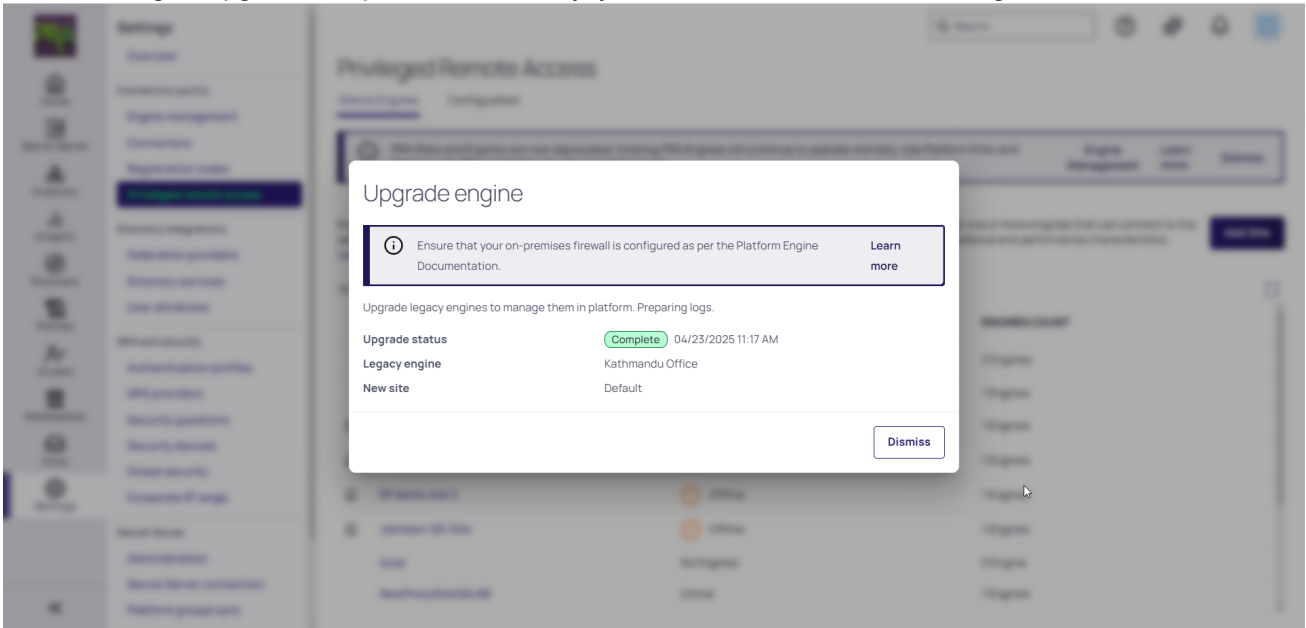



Note: You have the option to dismiss this window while the standalone engine is being upgraded in the background. You can view the progress of the engine upgrade in the **Notifications** section:



Privileged Remote Access

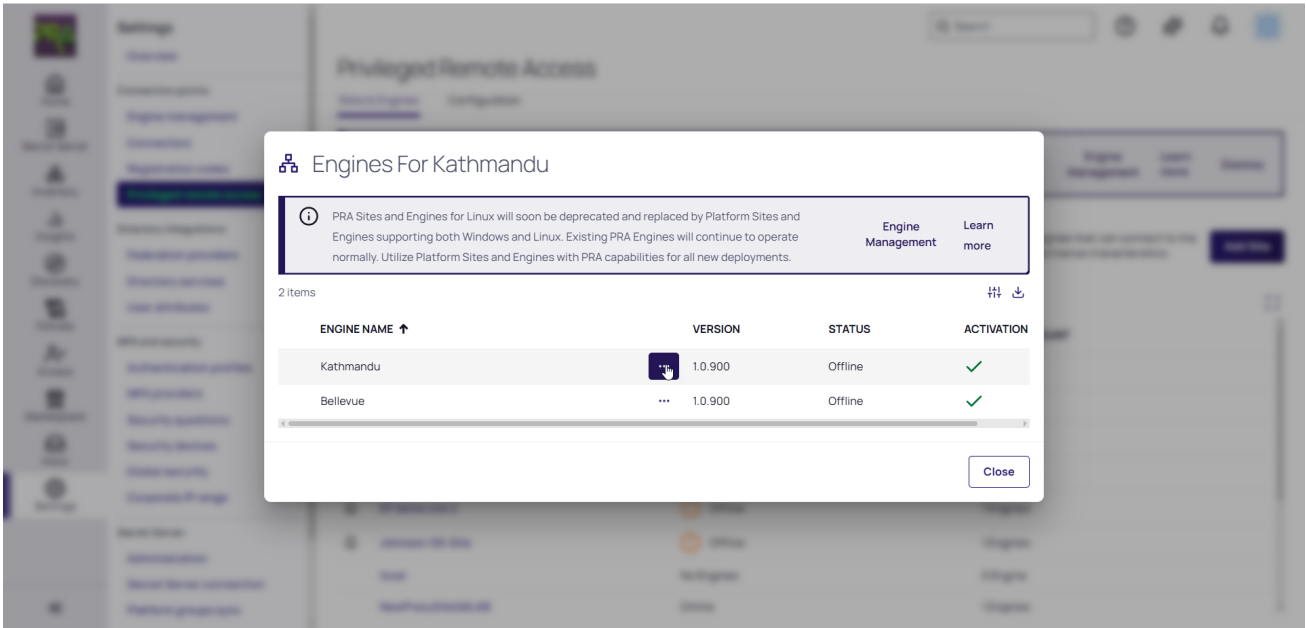
9. When the engine upgrade completed successfully, you will see a confirmation message like the one below:



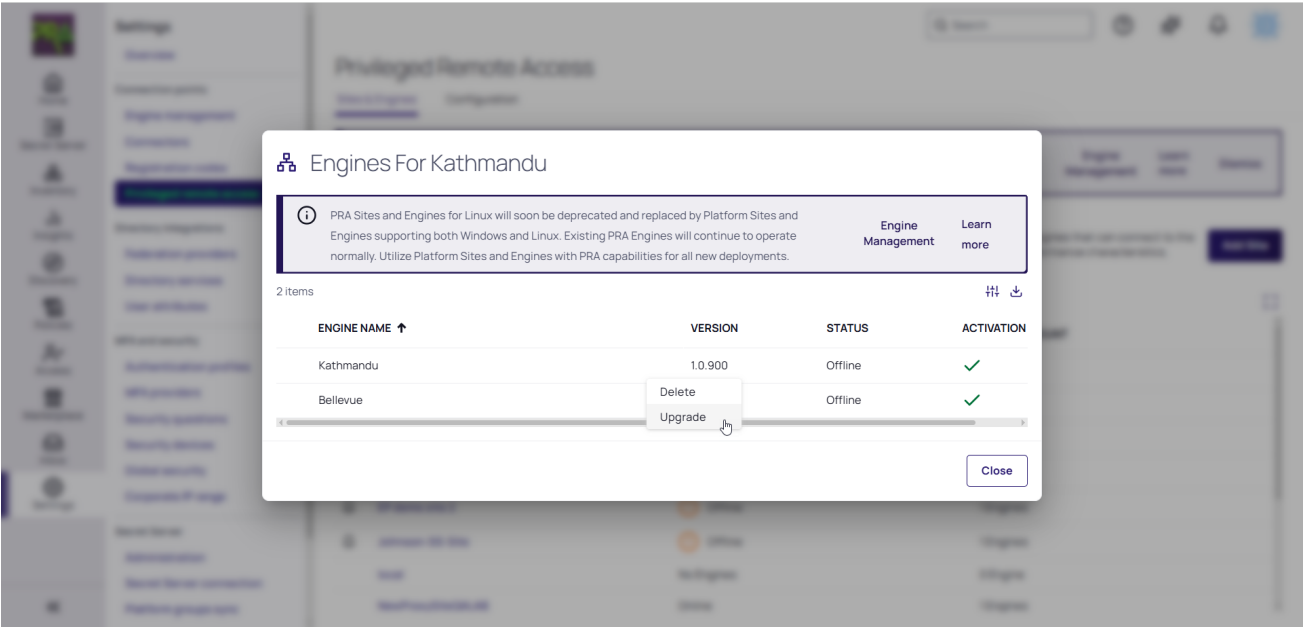
 **Important:** If the engine upgrade was not successful, click **Retry**. Alternately, you may also try to manually upgrade the engine as described below.

Manually Upgrading a Standalone PRA Engine to the platform Engine

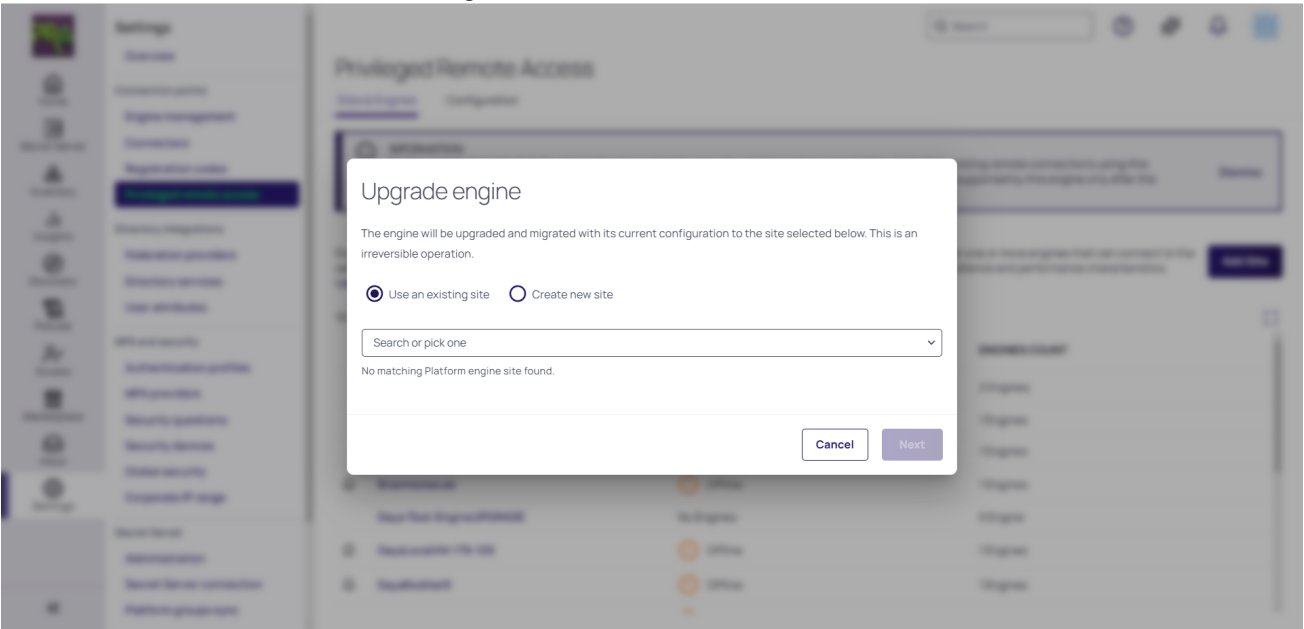
1. Click the "More Options" menu next to the engine




2. Click **Upgrade**.



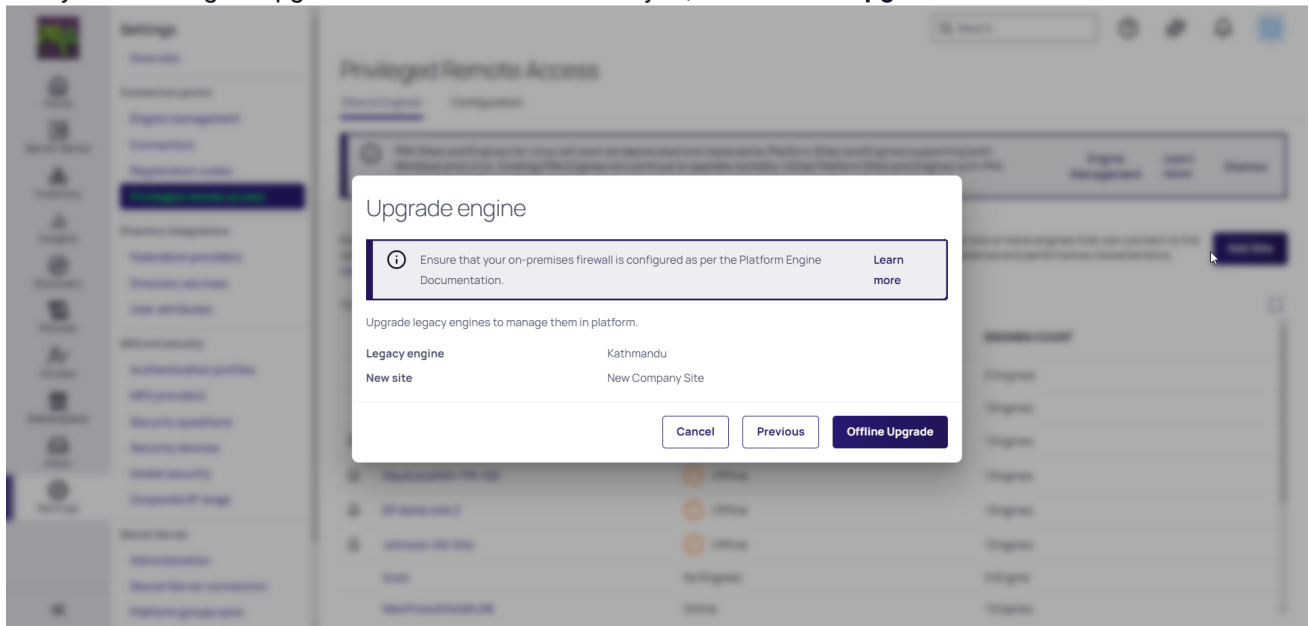
3. Select a Delinea Platform site for the engine and click **Next**.



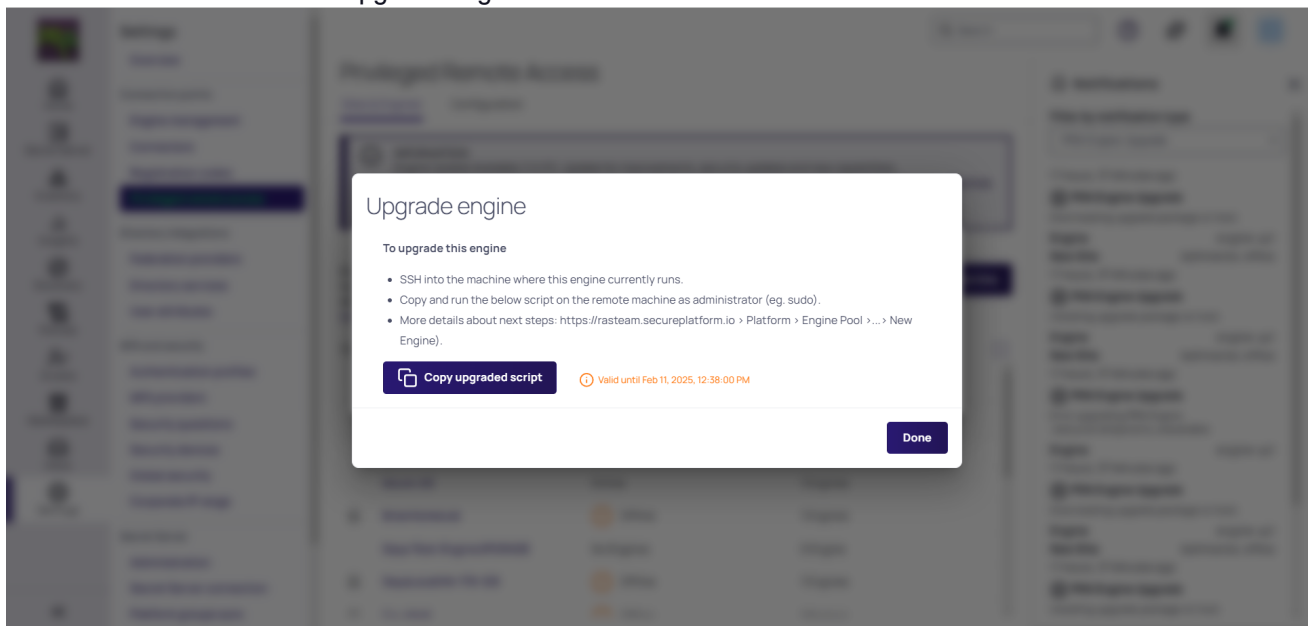
 **Note:** If a matching Delinea Platform site is found, it will be automatically pre-selected. You also have the option to create a new Platform site.

Privileged Remote Access

4. Verify that the engine upgrade information is correct. If yes, click **Offline Upgrade**.



5. Follow the instructions in the upgrade engine window.



Important: When manually upgrading the engine, ensure the server is hosting the same standalone engine that is being upgraded.

Upgrading the Standalone PRA Engine While Working in an Active Session

When *upgrading* the legacy PRA engine to the Platform Engine, any existing remote sessions being tunneled through the engine, will be disconnected and the engine will not support any new connections for the duration of the *upgrade*.

Using the PRA Engine

Important: This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

This page tells how to use Privileged Remote Access (PRA).

PRA and the Delinea Platform

All PRA remote connections occur within a user's Delinea Platform UI session. If a user logs out or is logged out of their Delinea Platform UI session, for example when their maximum session time is exceeded, all active PRA remote connections are automatically terminated.

Delinea Platform users may be subject to Identity Policies that define inactivity time limits for browser-based sessions. Please note that activity in any PRA remote connection browser tab is also considered to be Delinea Platform UI activity and keeps a user's Delinea Platform UI session active.

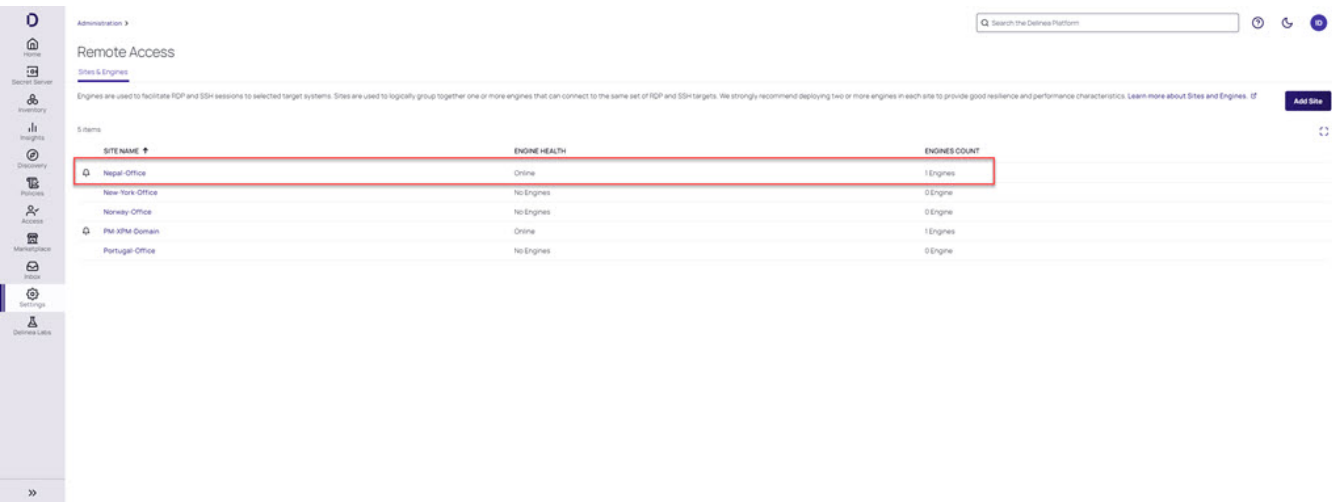
PRA Sites

A PRA Site is the location where local (on-prem) Windows and Linux resources are stored. A Site includes the engines to which these resources are available. For reliability, it is recommended to add at least two engines to each site.

PRA sites are mainly used on the launch secrets page, where users need to select a site from the list for the selected secret. Once the selection is made, an SSH or RDP connection will be established through any available engine of this site.

Naming a PRA Site

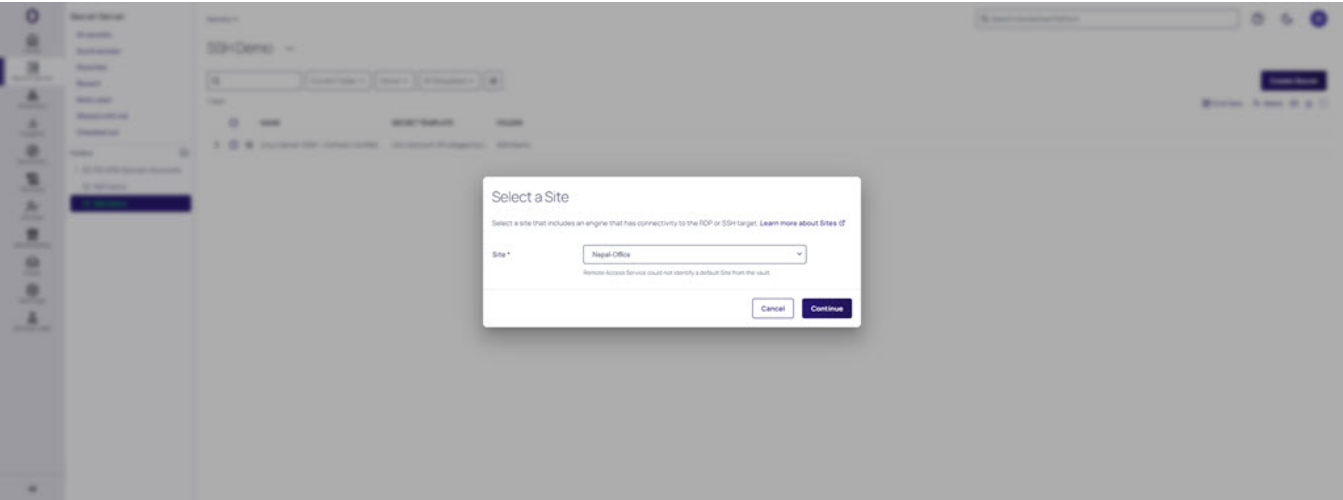
Delinea recommends that users name their PRA Sites for engines the same as the site used for the secret. This way, the site is automatically selected when launching a session and removes the necessity to manually search for a site to use for the session.




The screenshot shows the 'Remote Access' section of the Delinea Platform UI. It features a table with columns for 'SITE NAME', 'ENGINE HEALTH', and 'ENGINES COUNT'. The table lists five sites: 'Regal-Office' (Online, 1 Engine), 'New York-Office' (No Engines, 0 Engines), 'Norway-Office' (No Engines, 0 Engines), 'PRA xMn Domain' (Online, 1 Engines), and 'Portugal-Office' (No Engines, 0 Engine). The first row is highlighted with a red border. A sidebar on the left contains navigation icons for Home, Secret Center, Inventory, Insights, Discovery, Products, Access, Marketplace, and Settings. A search bar at the top right says 'Search the Delinea Platform'.

SITE NAME	ENGINE HEALTH	ENGINES COUNT
Regal-Office	Online	1 Engines
New York-Office	No Engines	0 Engines
Norway-Office	No Engines	0 Engines
PRA xMn Domain	Online	1 Engines
Portugal-Office	No Engines	0 Engine

Privileged Remote Access



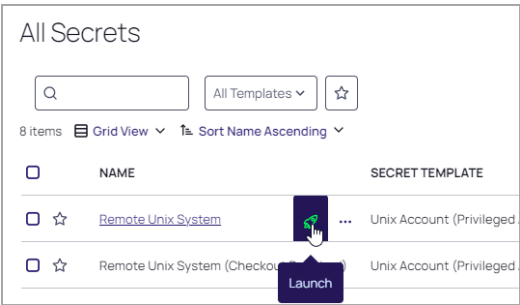
 **Note:** The site selection drop-down is only prompted if the PRA Site name and the site used for the secret do not match.

Launch a PRA Session

Delinea Privileged Remote Access (PRA) runs entirely on the Delinea Platform interface, enabling users to quickly access and control remote computers.

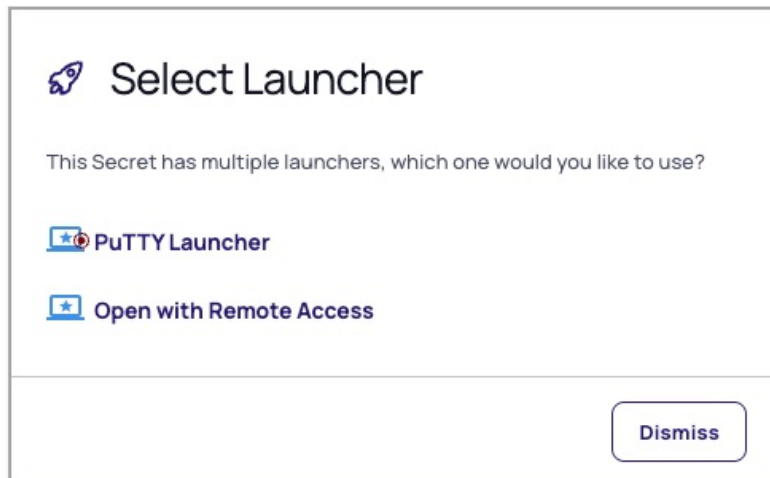
To launch a PRA session, follow these steps:

1. Log into the Delinea Platform.
2. From the left-side navigation, click **Secret Server** (or **Remote Access** for on-premises Secret Server).
3. Locate a secret associated with PRA .
4. Hover your cursor over the Secret row
5. Click the rocket (launch) icon.

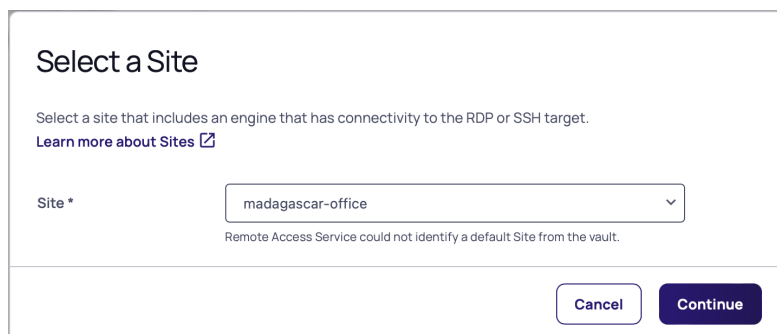



6. From the pop-up window, click **Open with Remote Access**.


Privileged Remote Access

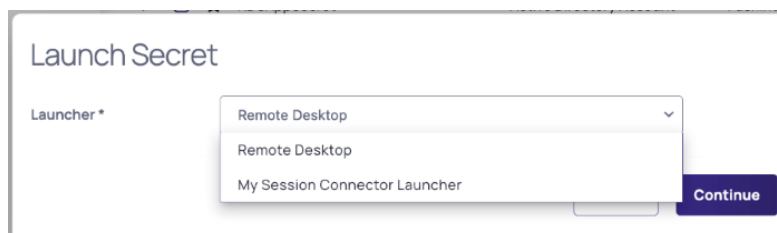


7. From the pop-up window, select the appropriate site from the drop-down menu and click **Continue**.




 **Note:** If a PRA Site name matches the vault Site name set on the Secret, the PRA Site is pre-selected in the Site Selection dialog. The site selection list is only shown when more than one PRA site exists to select from.

 **Important:** If you have Session Connector based launchers associated with a secret template, you will see a second dialog window where you will be able to select the session connector launcher. For more information on how to set up a Session Connector, please refer to the [Session Connector documentation](#).





From Secret Server On-Premises

 **Important:** When using Privileged Remote Access (PRA) with Secret Server On-Premises, any restrictions such as checkouts, checkout with tickets, approval workflows, quantumlock, etc. must be fulfilled directly in the Secret Server On-Premises UI. These must be completed prior to initiating remote access through PRA.

This section describes how to launch secure RDP or SSH PRA sessions from the Delinea Platform to remote protected resources using Secret Server On-Premises.

1. Log into the Delinea Platform.
2. From the left-side navigation, select **Settings > Remote Access**.
3. Locate the appropriate secret.
4. Click **Launch**.
5. Select the appropriate site from the drop-down menu and click **Continue**.




 **Note:** If a PRA Site name matches the Secret Server Site name set on the Secret, the PRA Site is pre-selected in the Site Selection dialog when the tenant has multiple Sites during the launch process.

6. A remote web session will launch in a new browser tab.

Update PRA Engines

Delinea frequently releases new versions of the PRA on-prem engine. Administrators receive notifications through the platform UI that engine updates are available, as shown below. These notifications can be ignored with no negative consequences.

When a PRA engine update is in progress, current sessions are not affected, but no new sessions can be started until the update is complete.

 **Note:** If your Delinea PRA engine version is lower than version 0.0.21, you must update it by manually uninstalling the older engine and then manually installing the newer one (see **Manually Updating a PRA Engine**, below). If your Delinea PRA engine is version 0.0.21 or higher, you can continue to the next section, **Updating a PRA Engine**.

Updating a PRA Engine

1. From the left navigation menu click **Settings**, then select **Remote access**
2. On the Sites & Engines tab, you can see the following:
 - The sites, listed under **Site Name**
 - The state of each site's engines under **Engine Health**
 - The number of engines on each site, under **Engines Count**.

Remote Access

Secret Server Connection

Secret Templates

Sites & Engines

INFORMATION




Engine Update Available (0.0.22). Update now for added capabilities, improved performance, and vulnerability fixes. Existing remote sessions will not be disrupted, however new sessions will be unable to launch.

Dismiss

Add sites and engines to be used to proxy RDP and SSH sessions. Users will be able to select the network before initiating a proxy session. Note that an engine must belong to a network, but can be removed or moved as needed. Networks for engines will show up here when installed on a remote network. We strongly recommend adding more than one engine per site.
[Learn more about Sites and Engines.](#)

+ Add Site

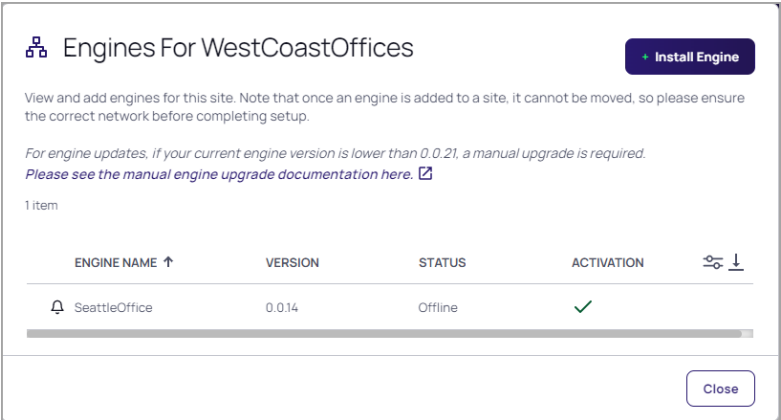
2 items

SITE NAME ↑	ENGINE HEALTH	ENGINES COUNT
 Azure	Online	1 Engines
 WestCoastOffices	 Offline	1 Engines

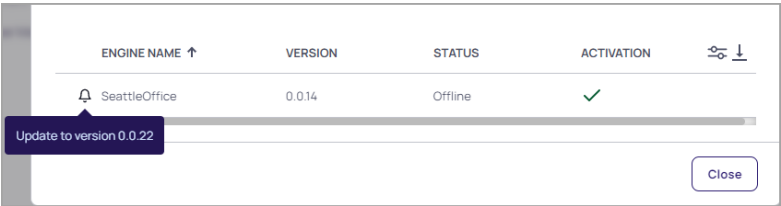
If one or more of your PRA engines is due for an update, you will see the following:

- A purple banner near the top of the page announcing the version number of the available update.
 - A bell icon to the left of each site containing one or more engines that can be updated.
 - A pop-up message when you click the bell, saying *There is a newer version of the engine available for this site. Please update soon!*
1. Click the name of the site where you wish to update an engine. The Engines page displays the engine's name, current version, status, and activation status.

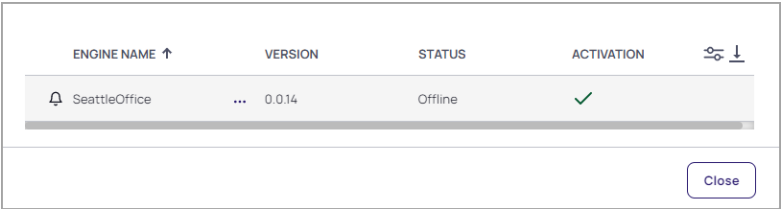
Privileged Remote Access



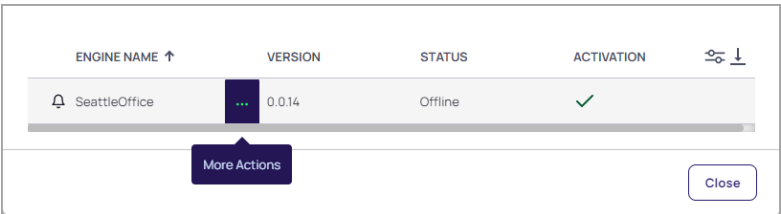
2. To see the version number of the newer engine you can update to, hover your cursor over the bell icon.



3. To update the engine, hover your cursor in the engine row. On the right side of the Engine Name column, three dots appear



4. Hover your cursor over the three dots. A pop-up appears saying *More Actions*.



5. Click the three dots and choose **Update**.

Privileged Remote Access

ENGINE NAME ↑	VERSION	STATUS	ACTIVATION	⚙️ ↓
🔔 SeattleOffice	0.0.14	Offline	✓	
<div>Update</div> <div>Delete</div> <div>Close</div>				

As the engine is updating, a daisy icon will appear in place of the bell. When a PRA engine update is in progress, current sessions are not affected, but no new sessions can be started until the update is complete. When the update completes, a check mark appears inside a circle, and if it fails, a bar appears inside a circle.

Manually Updating a PRA Engine

To manually update a PRA engine, follow these steps:

1. Uninstall the engine by completing the steps in the [Uninstall](#) section.
2. Once the engine is uninstalled, follow the procedure in [Installing a Remote Access Engine](#) to install the most recent version of the PRA on-prem engine.

Accessing Remote Applications With PRA

Remote applications allow users to establish connections to desktop applications on remote Windows servers, enabling VPN-less access from any location with an internet connection.

Prerequisites

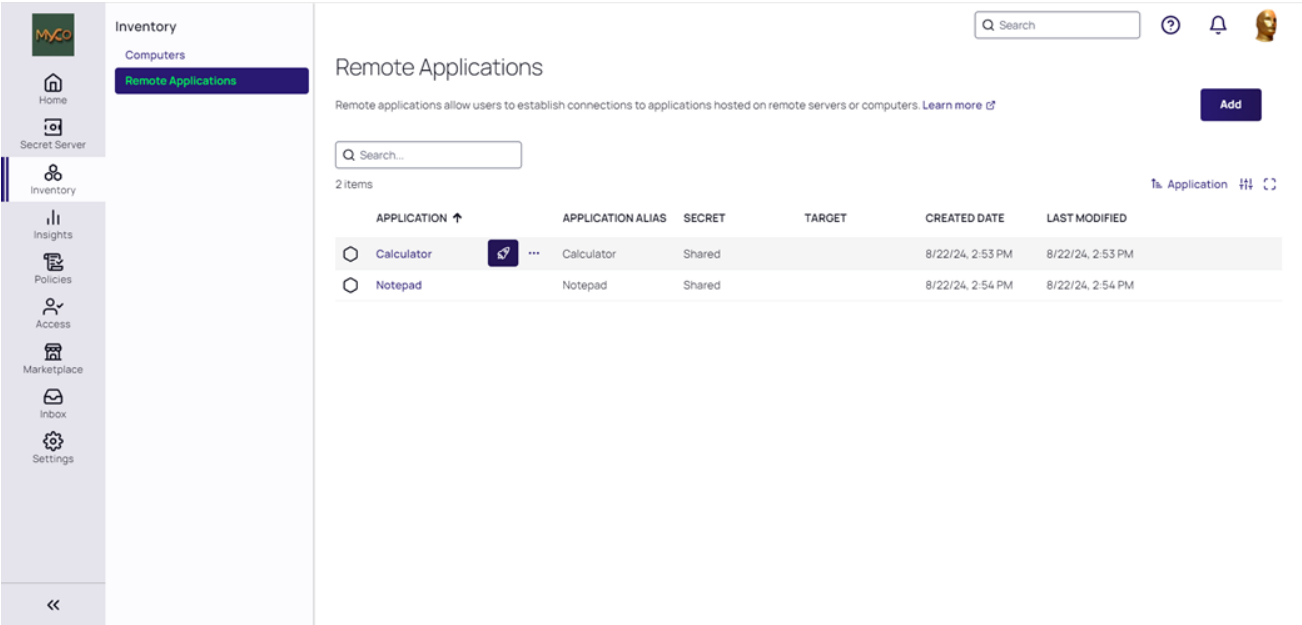
Administrators will need to ensure that users have the necessary permissions to launch RemoteApps. See "RemoteApp Permissions " on page 349 for more information.

For more information on how to setup RemoteApps on your Windows infrastructure, please refer to the [Microsoft documentation](#).

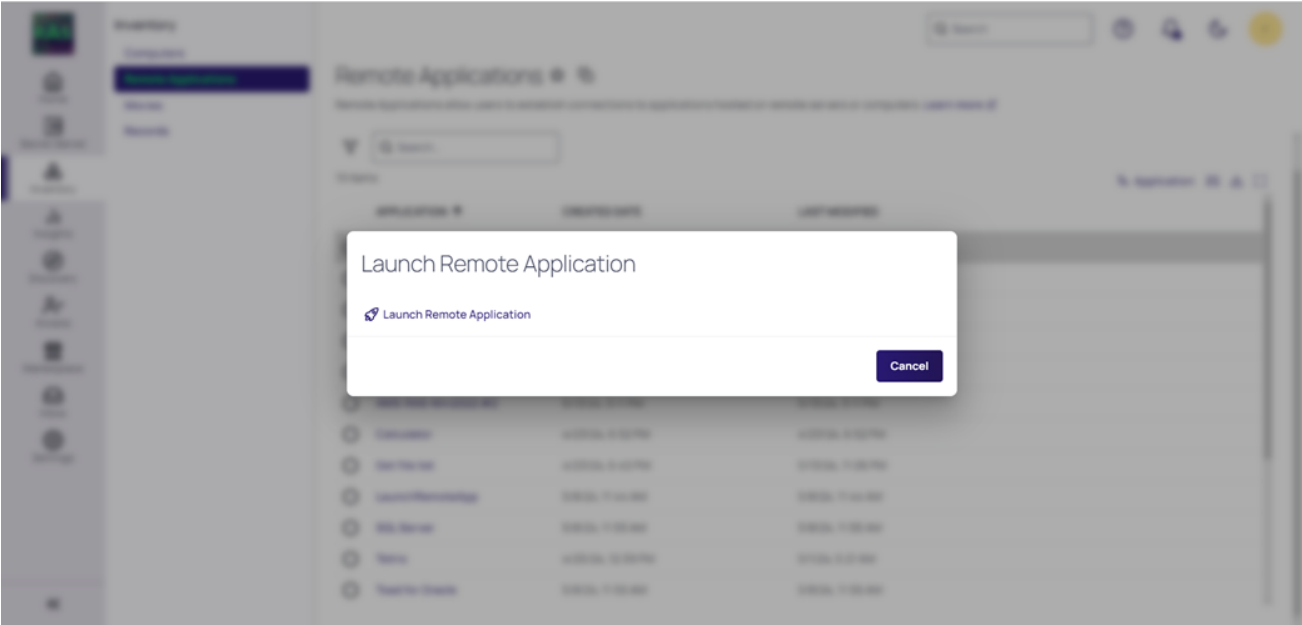
Launch a Remote Application


1. Navigate to **Inventory > Remote Applications**
2. Click the launch icon next to the secret name:

Privileged Remote Access




3. Click **Launch Remote Application**



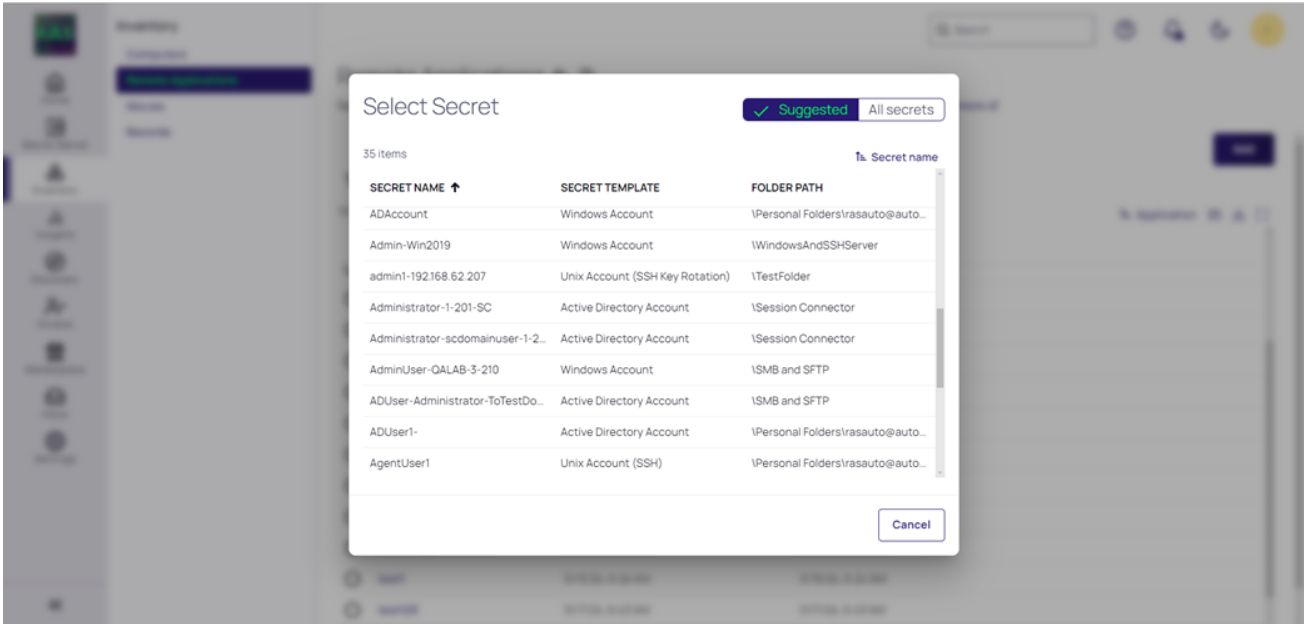
 **Note:** After clicking Launch Remote Application, you may be asked to select a target machine if one was not specified when the remote application was created

4. Set a secret associated with the remote application.

 **Note:** This is only necessary if no shared secret was associated with the remote application when it was created.



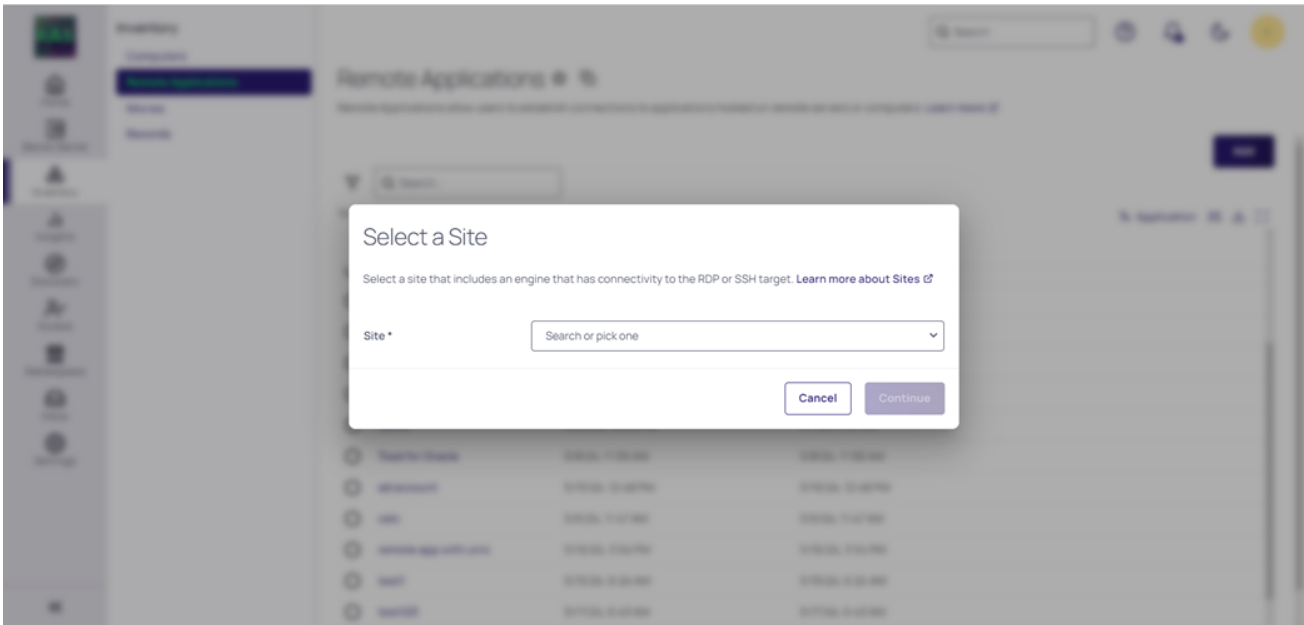
Some types of secret templates include *Machine* fields that refer to one or more target hosts (e.g. the Windows Account template). If a user selects such a secret with a Remote App, PRA will ignore any configured target host asset and attempt to launch the remote application on the target host specified in the secret.



5. Select a site and click **Continue**

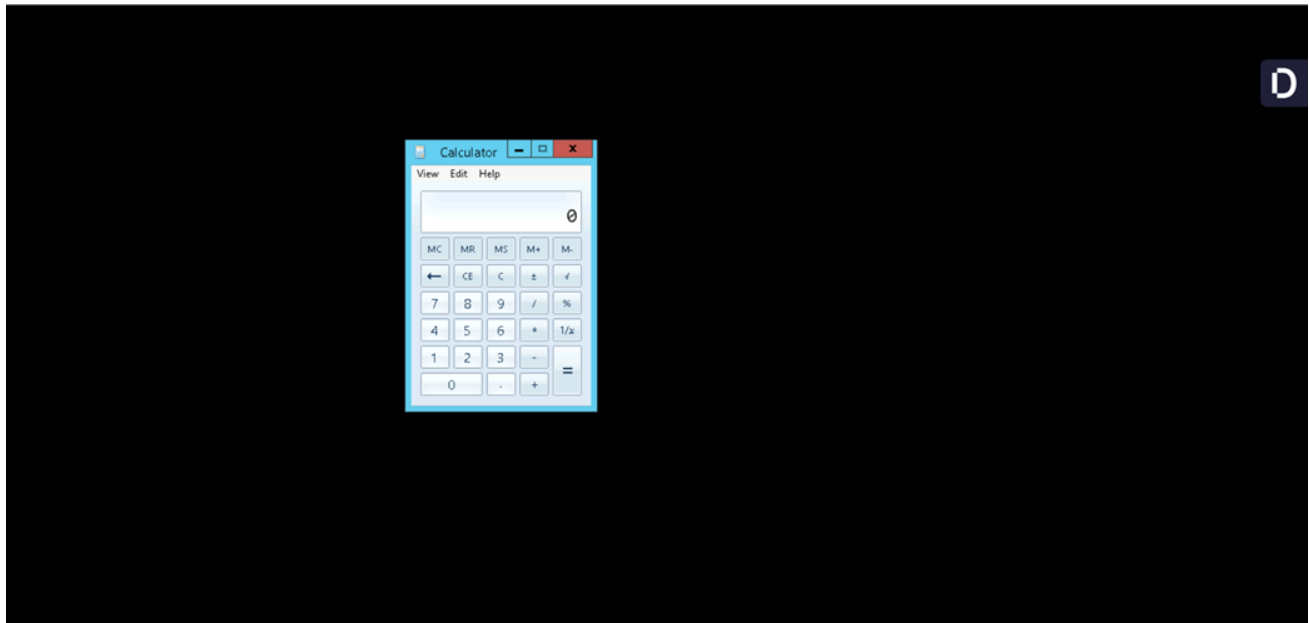


Note: You will be asked to select a site only if a PRA site with the same name as the site on the secret does not exist, or if the site exists but no active engine is deployed to the site.



Privileged Remote Access

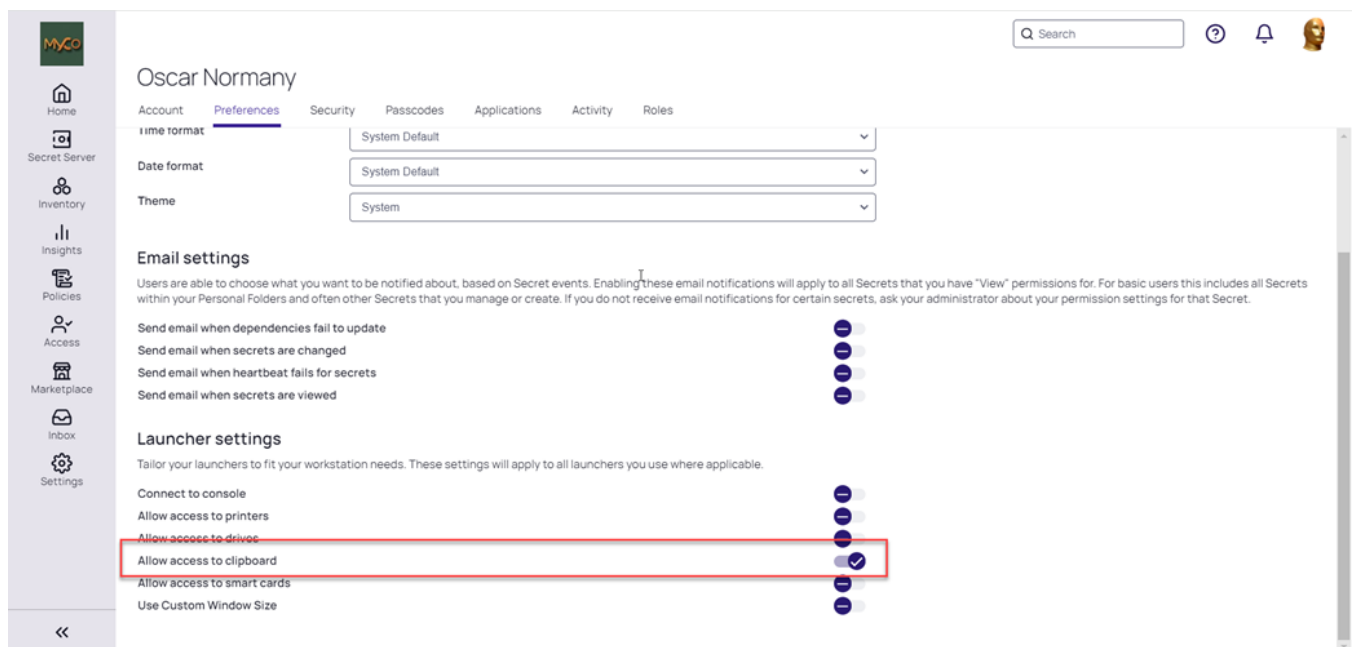
- The remote application has been successfully launched. In this example, the RemoteApp is the Calculator app.



- You may disconnect or logout from the remote application when you are done. Please see the [Delinea Menu](#) help to learn more.




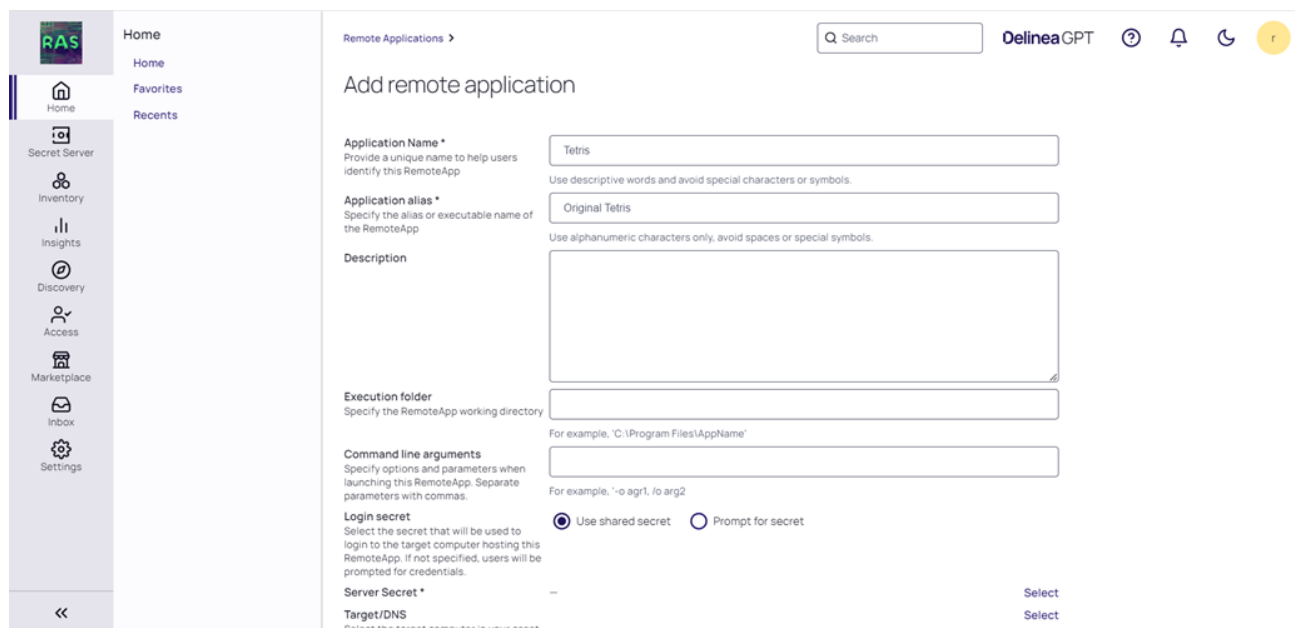
Note: A user's preferences for Launcher Settings found in **Account Details > Preferences** is used to control Clipboard access. Make sure this toggle is configured to *True* if you need to use the clipboard functionality. Similar permissions may be needed in a *secret* as well.



Add a New Remote Application


1. Navigate to **Inventory > Remote Applications**
2. Click **Add**
3. Fill in all of the required fields marked with an asterisk and other fields, if needed.


 **Important:** The *Application Alias* must match the application's remotely published alias. Alternatively, you can also input the full file path to the remote application.



The screenshot shows the 'Add remote application' form in the Delinea GPT interface. The form is titled 'Add remote application' and is located under the 'Remote Applications' section. The form includes the following fields and options:

- Application Name ***: Provide a unique name to help users identify this RemoteApp. (Text input: Tetris)
- Application alias ***: Specify the alias or executable name of the RemoteApp. (Text input: Original Tetris)
- Description**: Use alphanumeric characters only, avoid spaces or special symbols. (Text area)
- Execution folder**: Specify the RemoteApp working directory. (Text input: For example, 'C:\Program Files\AppName')
- Command line arguments**: Specify options and parameters when launching this RemoteApp. Separate parameters with commas. (Text input: For example, '-o arg1, /o arg2')
- Login secret**: Select the secret that will be used to login to the target computer hosting this RemoteApp. If not specified, users will be prompted for credentials. (Radio buttons: ☒ Use shared secret, ☐ Prompt for secret)
- Server Secret ***: (Text input: --) (Select button)
- Target/DNS**: Select the target computer in your asset. (Text input: --) (Select button)

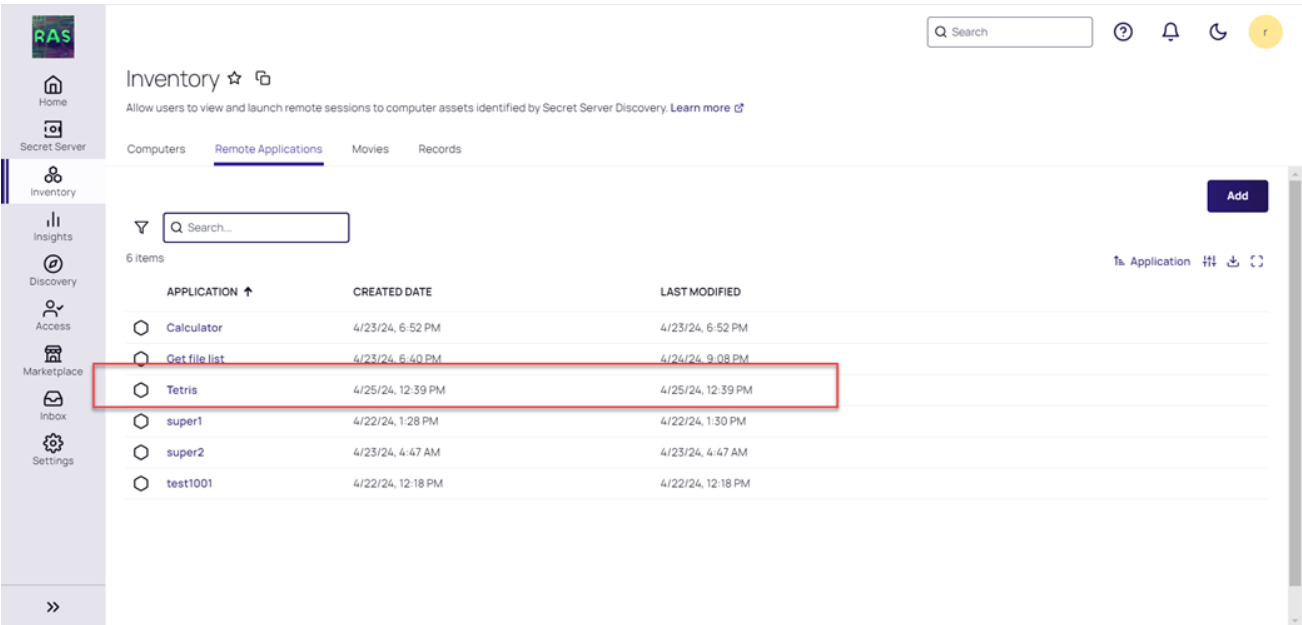
 A pre-selected shared secret may be used to create a remote application when the RemoteApp host machine needs to be accessed using the same credentials shared across all users. Please note that users launching this RemoteApp will need at least *View* permissions to that secret in order to access the pre-selected secret. If users require user-specific secrets to connect to the RemoteApp host, then this field can be left empty. When users launch the RemoteApp, they will be prompted to select a secret.

 When configuring a RemoteApp to prompt for a secret, users are required to select a computer from their asset inventory.

4. Click **Save**.

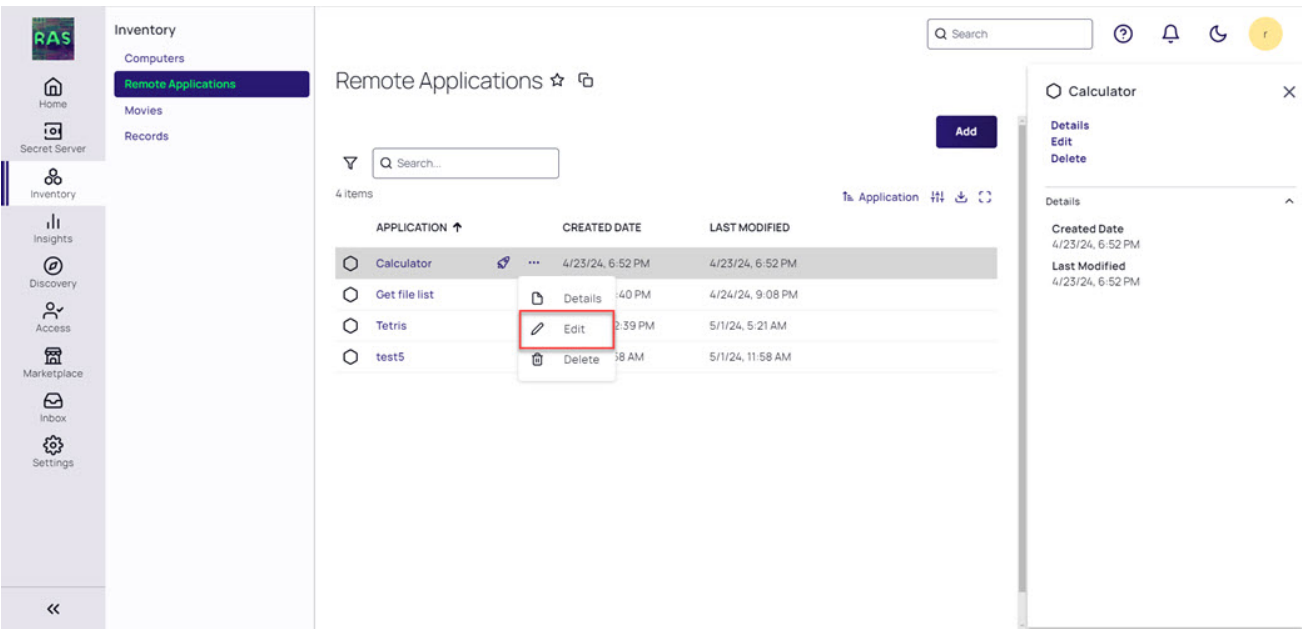
Privileged Remote Access

5. Your remote application is now created



Edit a Remote Application

1. Click the three dots menu and select **Edit**



2. The **Edit Remote Application** screen appears:

Remote Applications >

Q Search

Edit remote application

Remote applications allow users to establish connections to applications hosted on remote servers or computers, enabling seamless access from any location with an internet connection. [Learn More](#)

Application Name *
Provide a unique name to help users identify this RemoteApp
Calculator
Use descriptive words and avoid special characters or symbols.

Application alias *
Specify the alias or executable name of the RemoteApp
win32calc
Use alphanumeric characters only, avoid spaces or special symbols.

Description
Windows calculator app

Execution folder
Specify the RemoteApp working directory
For example, 'C:\Program Files\AppName'

Command line arguments
Specify options and parameters when launching this RemoteApp. Separate parameters with commas.
For example, '-o arg1 /o arg2'

Server secret *
Select the secret that will be used to login to the target computer hosting this RemoteApp. If not specified, users will be prompted for credentials.
None [Select](#)

Target/DNS
Select the target computer in your asset inventory that has been configured as the RDS host for this RemoteApp
[Select](#)

[Cancel](#) [Save](#)

Using the Delinea Menu

When a user successfully initiates a remote connection, they will see a Delinea menu on the right side of the screen:



This menu consists of the following options:

1. Transfer files
2. Session information
3. Settings
4. Screenshot
5. Clipboard
6. Enter full screen
7. Disconnect



Note: The Delinea PRA menu can be activated using Ctrl-Alt-Shift when keyboards need to be used for accessibility reasons. Users can tab through the menu selections and hit Enter to activate any menu action

A more detailed description of each menu item can be found below.



Transfer Files

For more information about file transfers, please see "Transferring Files With PRA " on page 334.



Session Information

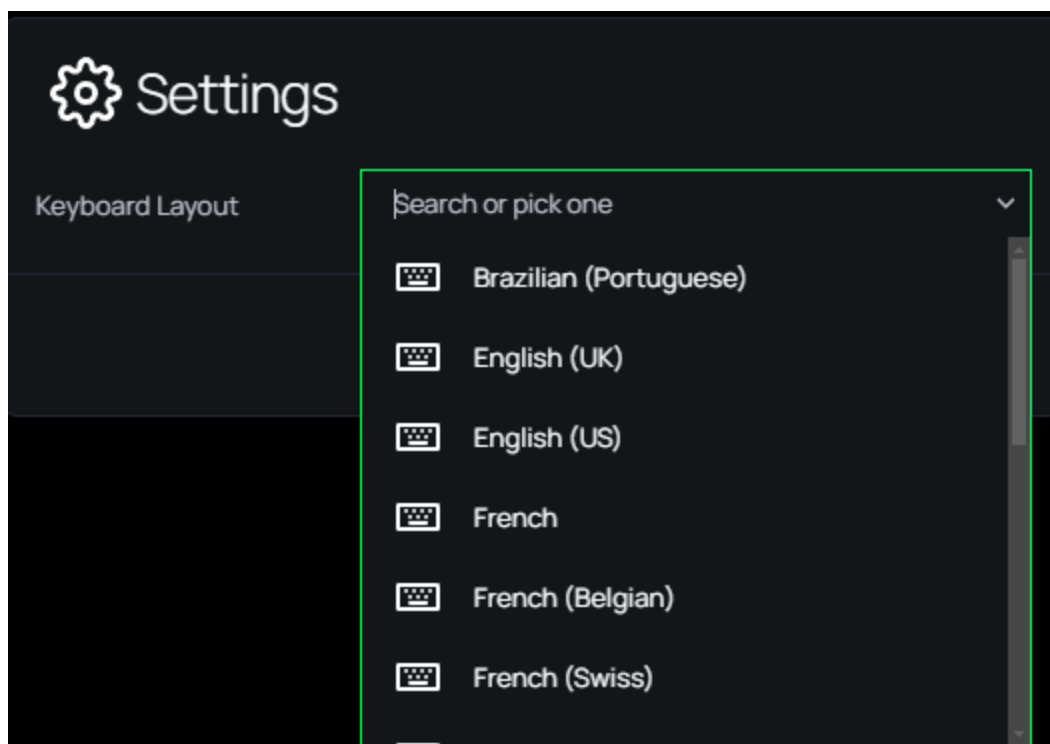
Session Information allows users to get some quick information on their current PRA connection which can be useful for diagnostic purposes during troubleshooting. It shows the:

1. Host name - Target machine's IP address or DNS name.
2. Site name -Name of the site where the target is deployed.
3. Engine name - The engine used to connect the PRA session.
4. Credential type - Specifies whether the credentials used were from the Secret Server vault, specified manually, or used the user's own account.
5. Session recording status - Whether session recording has been enabled or disabled.
6. Session start time - How long ago was the session initiated.



Settings

The **Settings** menu option allows users to easily switch their keyboard layout to match their language-specific preference. The drop down in the screenshot shows some of the currently supported languages/layouts.



The selected keyboard layout will be saved for all tenant users. When a user changes their preferred keyboard configuration after connecting to a remote machine with PRA, their preference will be remembered and applied every time that specific target machine is used. The keyboard setting is locked-in until a user changes it.



Note: Changing the keyboard layout requires PRA to disconnect and reconnect with the target system. This is currently **not** supported when connecting to a target through a secret that has **proxy enabled**. In such cases, the user will need to **manually connect again** to the target after automatic reconnect fails.




Screenshot

If a user clicks the **Take Screenshot** icon, PRA will automatically take a screenshot of the user's remote session and download the file to their local machine.



Clipboard

The **Clipboard** functionality allows users to copy and paste text between their local machine and the remote target. Simply paste the text into the **Clipboard** window and click **Send to Server Clipboard**. Remote clipboard content is also automatically copied into the clipboard.


 **Important:** The permissions for the clipboard are currently controlled in the secret's RDP Launcher configuration, and all user clipboard actions (read, copy, paste) are logged in the Delinea Platform audit log.

The session clipboard buffer size is set to 256 KB. If you need to work with text larger than this limit, use multiple copy/paste operations or utilize the file transfer functionality. ([Learn more](#))

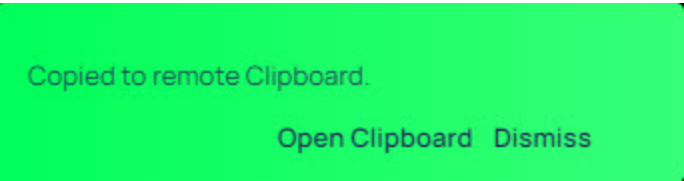
The table below describes keyboard shortcuts for text copy/paste operations.

Operation	Remote Target: SSH	Remote Target: RDP
Copy	Auto-copy on select	Ctrl + C
Paste	Ctrl + Shift + V	Ctrl + V

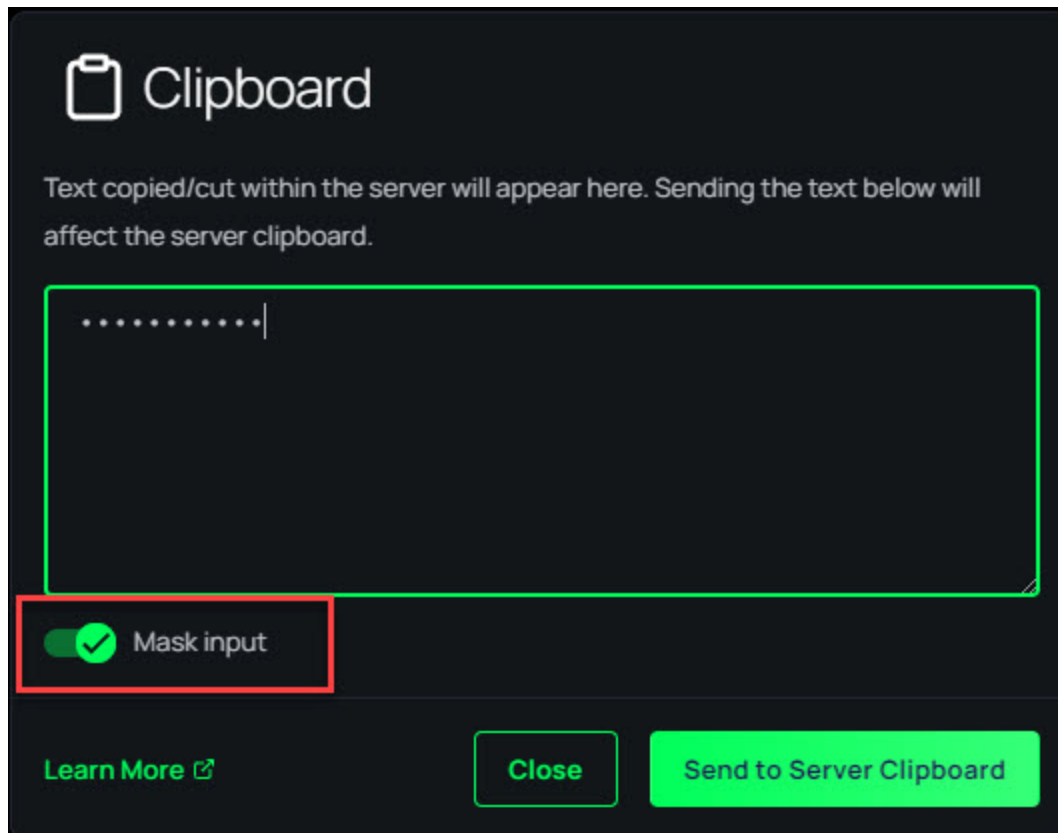
 **Note:** This functionality is only available on Google Chrome and Microsoft Edge browsers.


 **Important:** Use your client device's native keyboard shortcuts for all local copy/paste operations. For example, if you are using Chrome or Edge on a MacOS client device, use Cmd+C/Cmd+V for local copy/paste actions.

Click **Open Clipboard** to view any copied text.



If you need to copy a password or any other sensitive values to the clipboard in order to use it on the remote session clipboard, you can enable the **Mask Input** toggle.



 **Note:** PRA only supports unformatted text content with the clipboard.



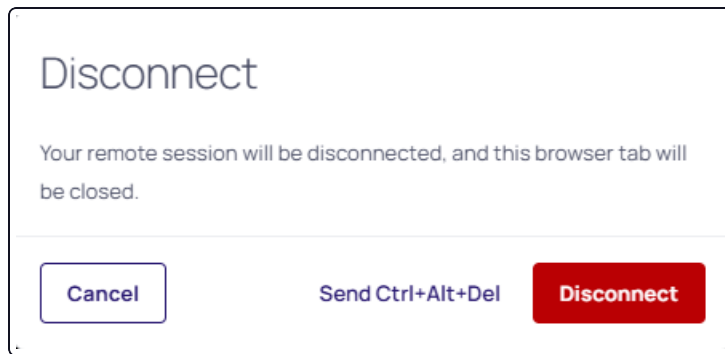
Enter Full Screen

The **Enter Full Screen** option allows the user to take advantage of all the space offered by their monitor. To exit out of full-screen mode, simply tap the icon a second time or click the *Esc* key on your keyboard.

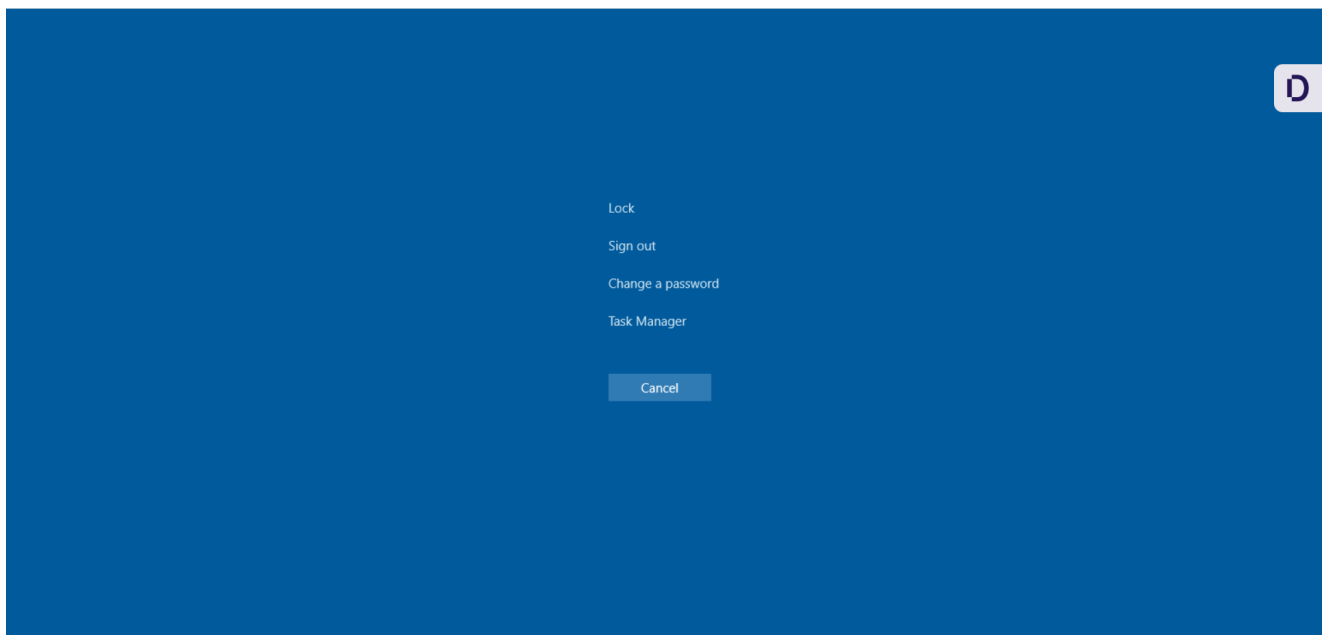



Disconnect

Clicking the **Disconnect** option will end the remote session and the browser window will be closed. Users can confirm their decision to disconnect or cancel to remain in the session.



Users have the option of logging out of the session by clicking the **Send Ctrl-Alt-Del** control. This normally opens up a dialog that presents Logout in addition to other options as configured on the target machine.:




 **Important:** For security best practices, please consider using Group Policy or Windows Registry settings to disable unintended access to the Task Manager or Password Changer options.

Transferring Files With PRA

Prerequisites

To enable file transfers to remote machines, the following prerequisites must be met:

1. An SFTP or SMB service must be running on the target machine. If both are enabled on the target machine, PRA will use SFTP.

 **Note:** For SMB file transfers, SMBV2+ is required.

Privileged Remote Access

2. Verify that the SFTP service is configured to use the standard port (22) and that appropriate permissions are granted to the user credentials used to connect remotely.
3. Verify that the SMB service is configured to use the standard port (445) and that appropriate permissions are granted to the user credentials used to connect remotely.

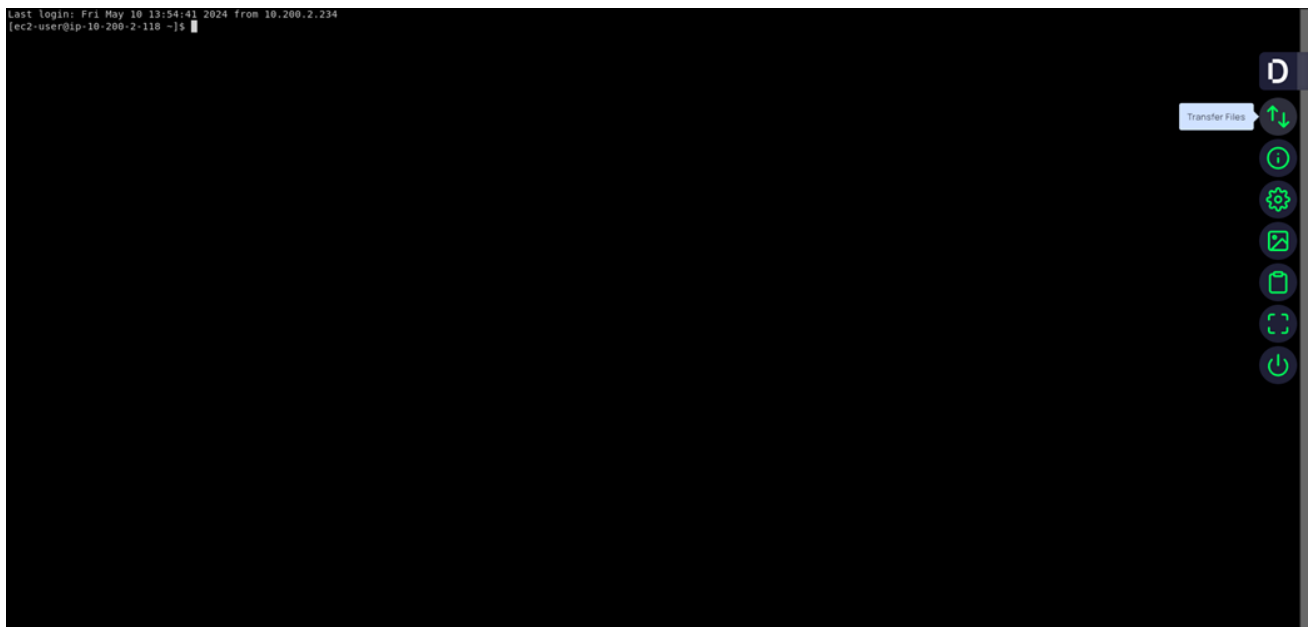
Verify that the SMB service is configured to use the standard port (445) and that appropriate permissions are granted to the user credentials used to connect remotely.

4. Please see [PRA Architecture](#) for additional pre-requisites.

Administrators will need to ensure that users needing to upload or download files have the necessary permissions. See "Understanding PRA Permissions and Roles" on page 346 for more information.

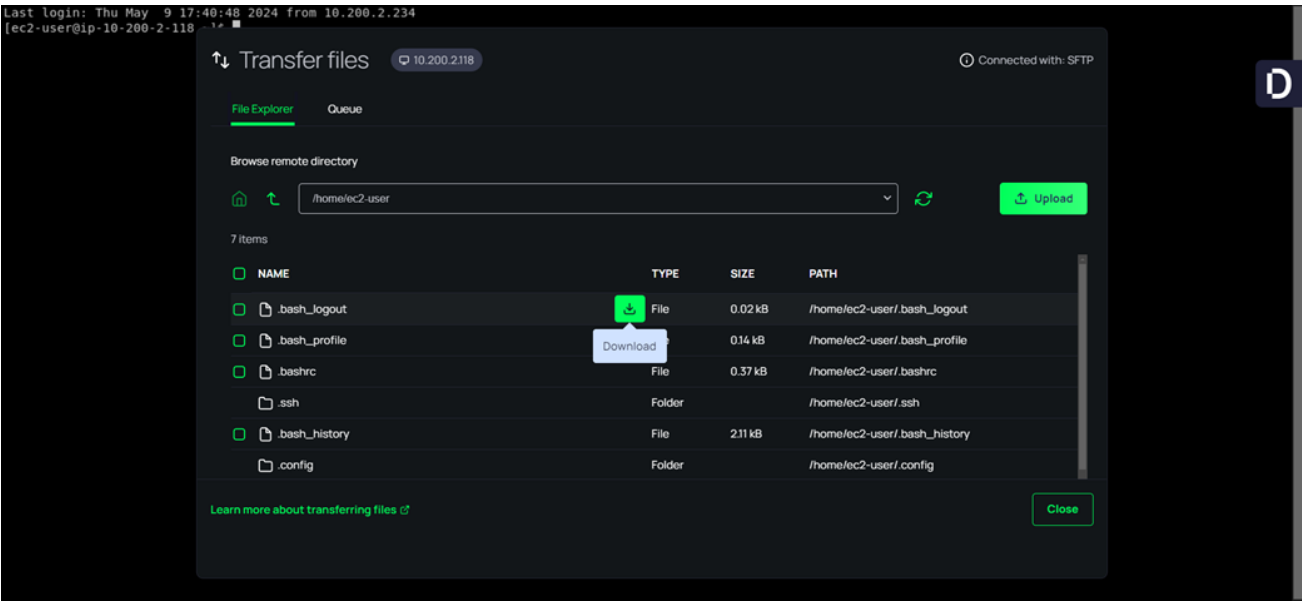
Download a File

1. Launch a PRA session to an SSH or RDP target. See [Launch a PRA Session](#) for more information.
2. Click on the floating menu on right side and click **Transfer Files**

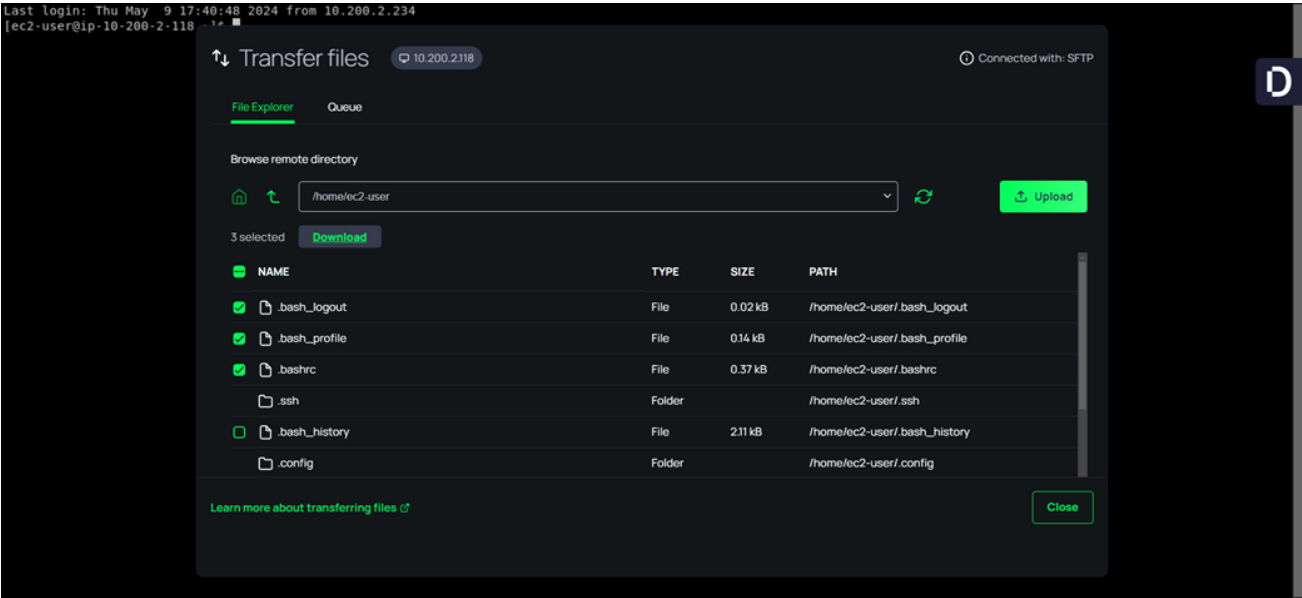


3. A modal dialog appears with files and an icon to download:

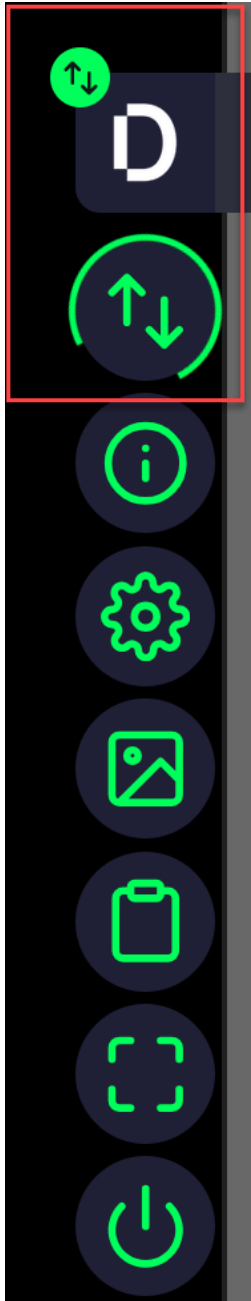
Privileged Remote Access





Users can click the download icon to quickly download a single file, or use multi-select and schedule multiple files to be downloaded.

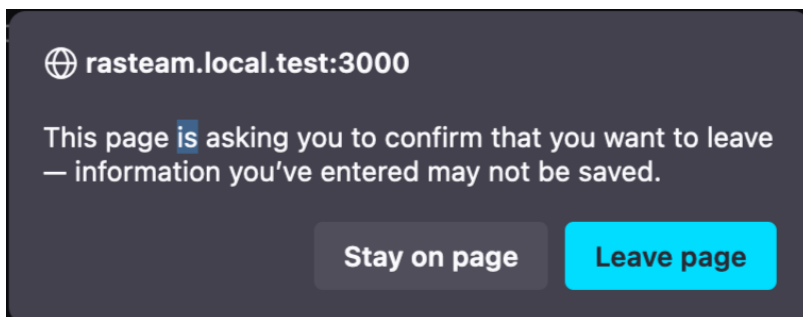


Users can close the file transfer window and continue to work with SSH/RDP connections while files are downloading in the background. The Delinea menu shows a transfer icon overlay while file transfers are in progress.



 **Note:** If you do not see a download icon, you do not have the necessary permissions to download the file.

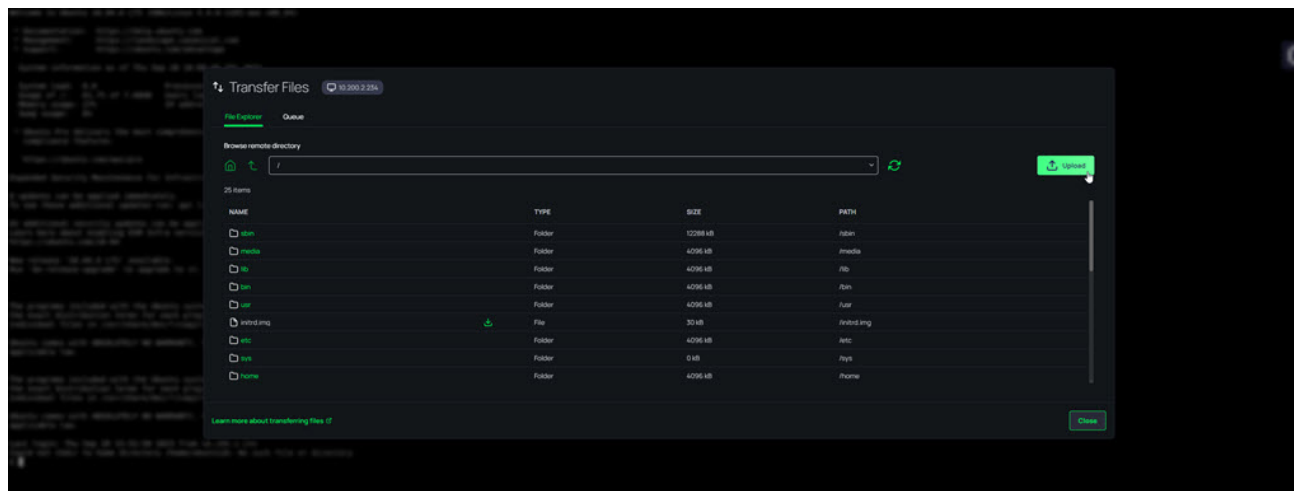
 **Note:** If a user tries to close the remote browser window or tab while file transfers are still in progress, they will see the following message alerting that file transfers are still in progress. This message may vary slightly across browsers and operating systems:



Upload Files

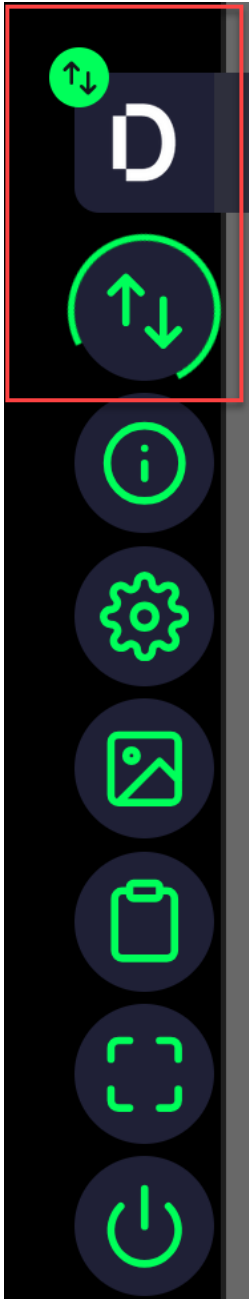
To upload files:


1. Launch a PRA session to an SSH or RDP target. See [Launch a PRA Session](#) for more information.
2. Click on the floating menu on right side and click **Transfer Files**.
3. Click the **Upload** button.




4. Users have the ability to select and enqueue multiple files for upload, with a limit of up to 500 files. Once enqueued, these files are displayed within the Queue tab for easy tracking. To maintain optimal performance, the system is configured to actively process up to 5 file uploads concurrently from the queue. Users can drag files into the “Browse remote directory” target area to upload files into the currently selected remote directory

Users can close the file transfer window and continue to work with SSH/RDP connections while files are uploading in the background. The Delinea menu shows a transfer icon overlay while file transfers are in progress.



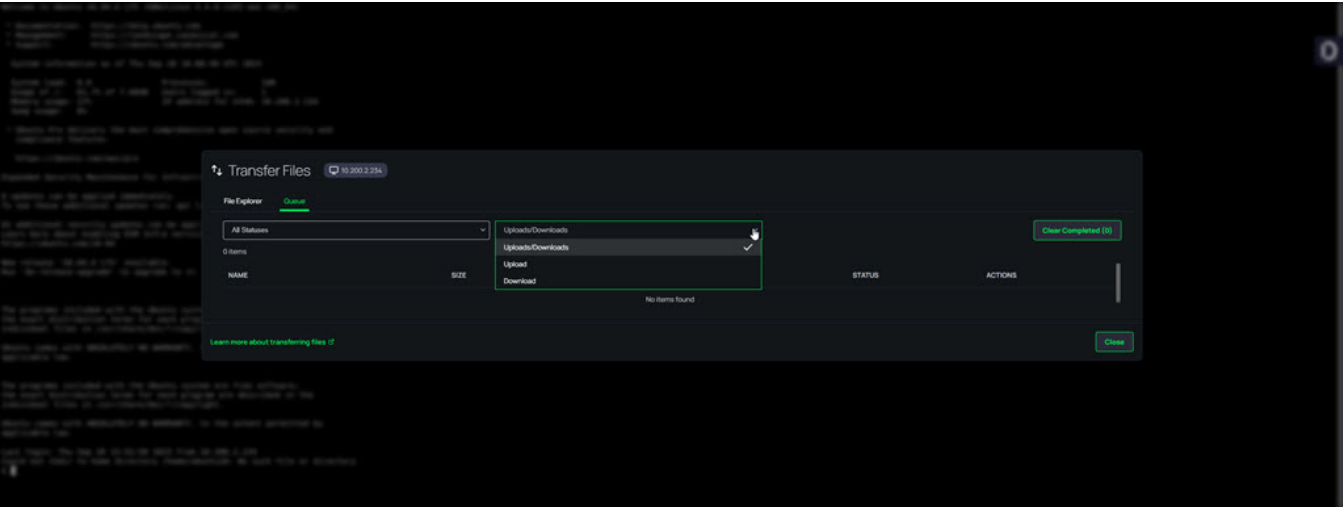
 **Note:** If you do not see an **Upload** button, you do not have the necessary permissions to upload files.

 **Note:** If you are using SMB and are trying to upload a file, please note that the root folder is not a valid target for upload or download.

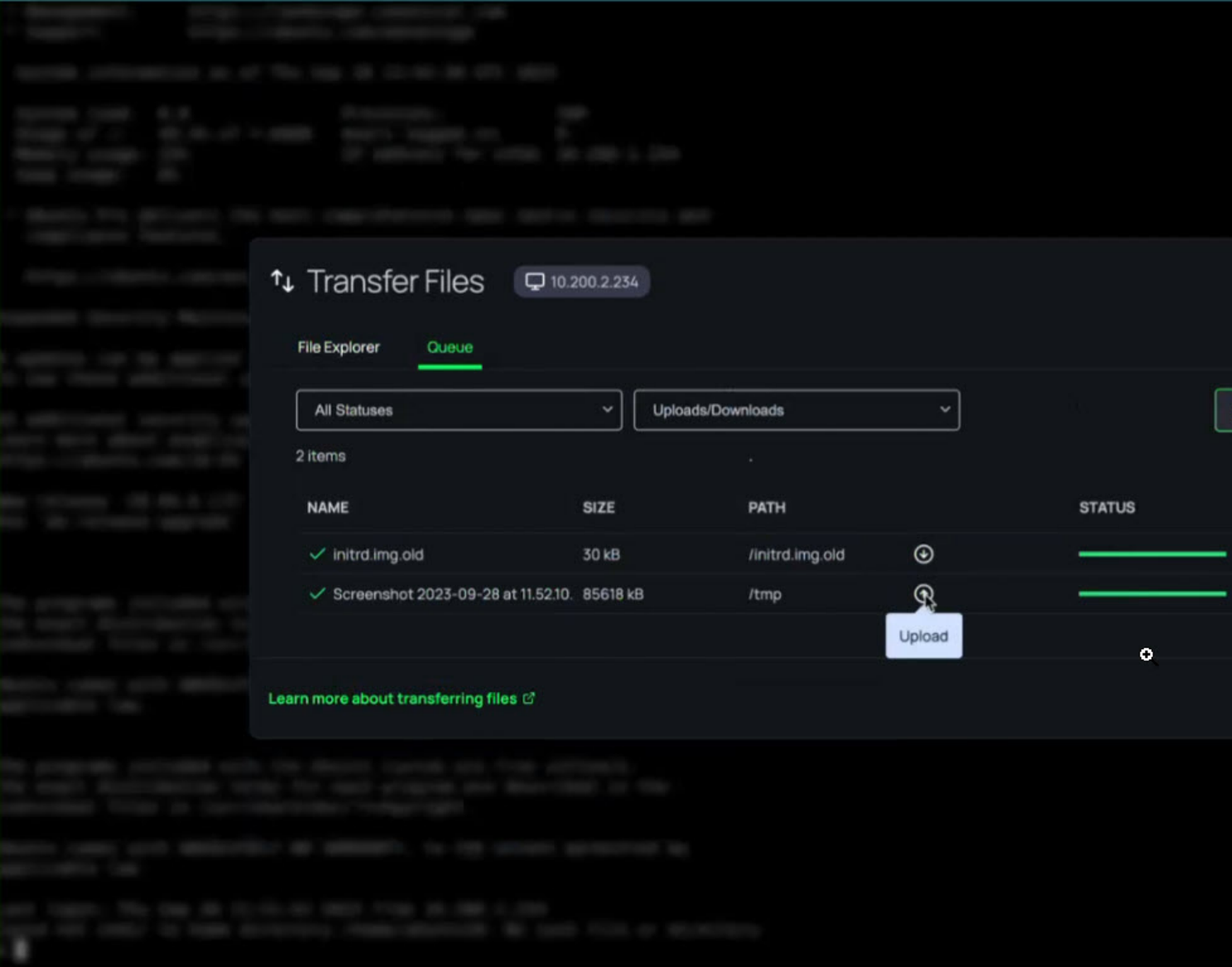
Queue Tab

Inside the Queue tab, you can monitor the progress of your file uploads and downloads by selecting the desired view the drop-down menu:

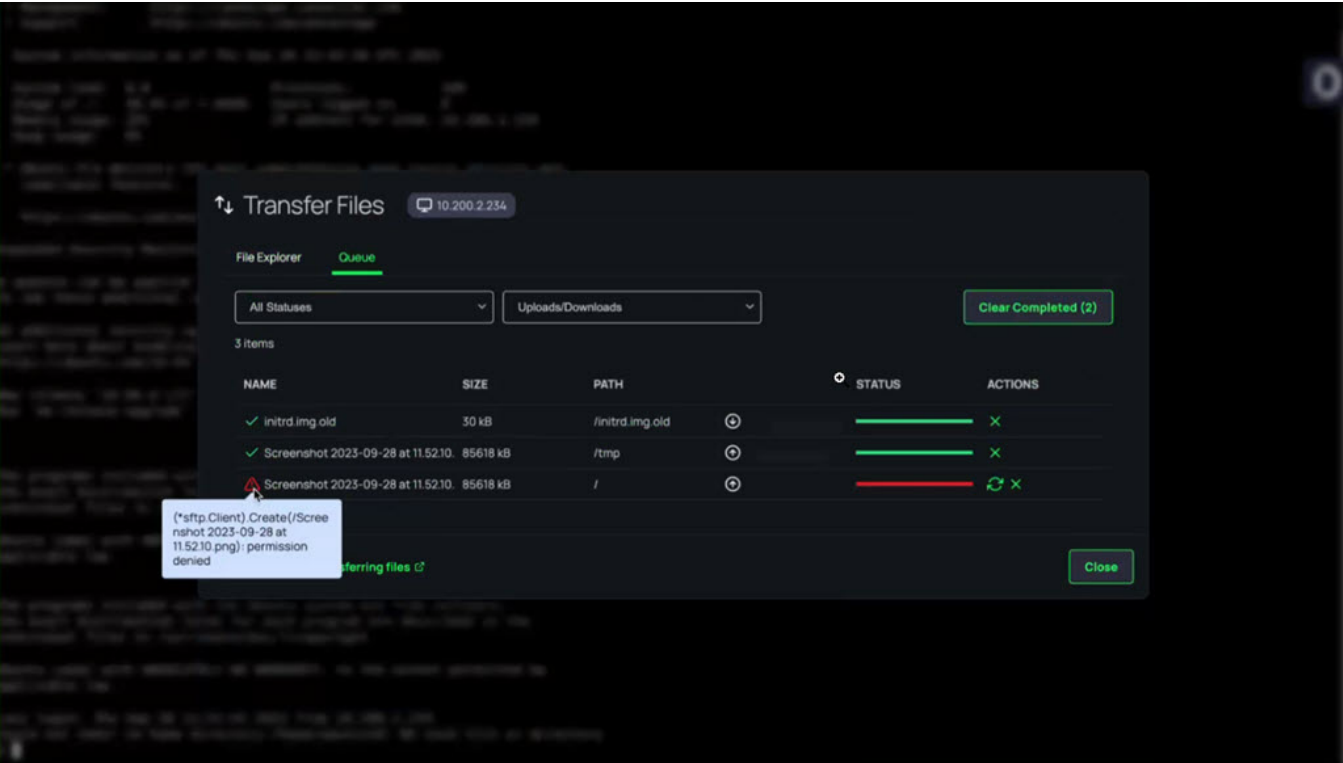
Privileged Remote Access



The system will show you the upload/download progress:



In the event of any failures, the system will display those as well along with an explanation:



Please note that file downloads are delegated to your browser, and depend on browser file download settings. As a result, the status shown in the Queue tab may be slightly different than what you see in your browser's file download messages and notifications.




For SFTP transfers with Windows targets, users can configure openssh-server or similar running on the default SFTP port (22)

Current Limitations

The following use cases are not supported:

- PRA Sessions that are opened via the Secret Server Distributed Engine Proxy.
- The target system has the Delinea Privilege Controls' agent/client installed with MFA enabled.
- Separate ports for SSH connections.
- Transferring files larger than 2048 MiB. Please note, that this can vary a little depending on metadata associated with the file
- SMB file transfers to SSH targets are not supported.

Accessing Private Web Applications With PRA

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.


Prerequisites

- Public web applications and web sites are not supported.
- Private web applications will not inject credentials into web applications/pages that have login forms. Use Web Password Filler with web template-based secrets to facilitate password injection in such cases.
- Private web applications require Platform Engines with PRA workloads. Deprecated standalone PRA engines are not supported.
- Administrators will need to ensure that users have the necessary permissions to launch Web Applications. See "Web Application Permissions" on page 350 for more information.


Creating a New Web Application


To create a new web application:

1. Navigate to **Inventory > Web Applications**.
2. Click **Add**.
3. Fill in all of the required fields marked with an asterisk.
 - Application name: Provide a unique name to help users identify this web application. The network address in the URL needs to be resolvable and reachable from the Platform Engine.
 - Private URL: The private-network based URL for the web application.

 **Important:** TLS certificates, if any, on private URLs are not validated.

- Public URL prefix: A unique prefix for the public URL to access this site. The unique prefix is used to create the corresponding public URL that will be used to access the private application without needing a VPN.

 **Important:** Add a prefix for the public URL so that your private web application can be reached by using a public URL like `https://prefix-tenantname.go.delinea.app`. The prefix must be unique so that the resulting URL is unique.

 **Important:** The prefix can only use a through z, 0 through 9 and _ (underscores). No other characters are allowed.

Privileged Remote Access

- **Site:** The Platform engine site for the location where your private web application is deployed.

The screenshot shows the 'Add web application' form in the Delinea console. The left sidebar contains navigation links: Home, Favorites, Recents, Dashboards (General, Analytics), Desktops, Summary, Secret Server, Inventory, Insights, Discovery, Policies, Identity Posture, Threat Center, Access, Marketplace, and Inbox. The main content area has a search bar and icons for help, settings, notifications, and user profile. The form fields are: Application Name (text input), Private URL (text input), Public URL prefix (text input with a dropdown for 'https://'), Description (text area), and Site (dropdown menu with 'Search or pick one'). At the bottom right are 'Cancel' and 'Save' buttons.

4. Click **Save**.

Launching a Web Application

To launch a web application:

1. Navigate to **Inventory > Web Applications**.
2. Click on the web application name. The Details page will open:

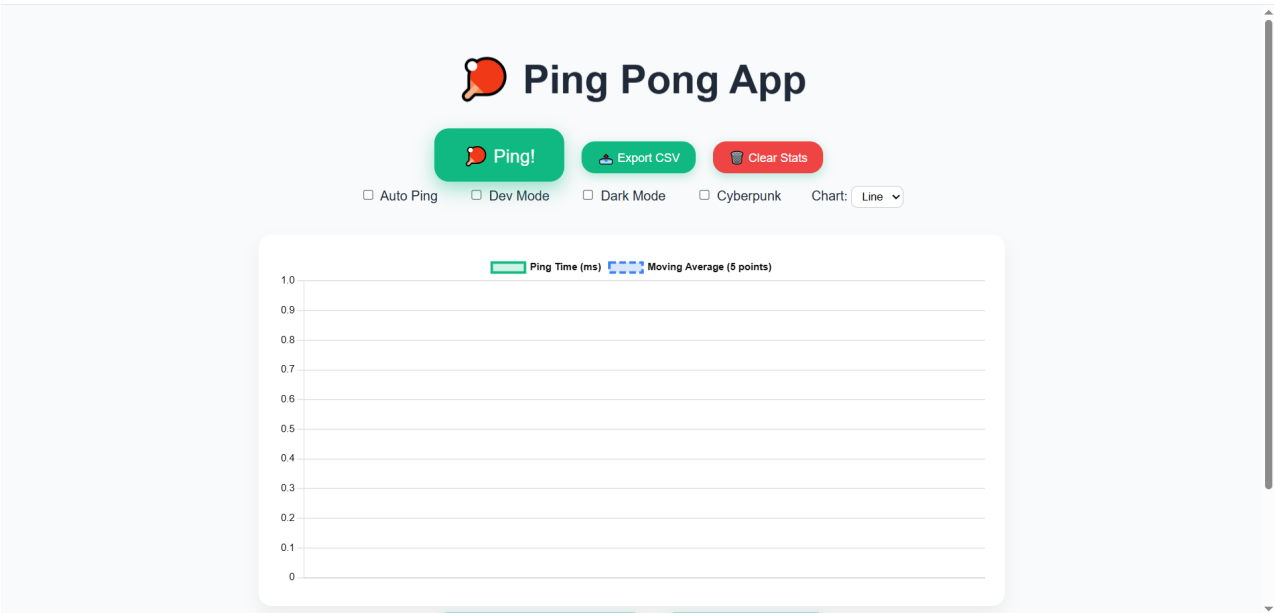
The screenshot shows the 'Web Applications' details page in the Delinea console. The left sidebar is the same as the previous screenshot, but with 'Web Applications' highlighted under 'Inventory'. The main content area shows the details for a web application named 'Ping!'. It includes a header with the application name, a star icon, and a dropdown menu. Below the header are buttons for 'Edit', 'Delete', and 'Launch'. The details section includes a table with the following information:

Details	
Name	Ping!
Description	Demo private web app
Private URL	http://myDevBox2:3000
Public URL	https://ping-pm-xpm-go.delinea.app
Site name	Azure

Below the table, there is a 'Launch web application' section with a 'Launch Web Application' button. At the bottom right, there are 'Created date' and 'Last modified' fields, both showing '7/1/25, 10:03 AM'.

3. Click **Launch Web Application**


4. The web application will launch.



You may also launch the web application from the list of application assets by clicking the launch icon:

The screenshot shows the Delve interface. On the left is a sidebar with various navigation icons. The main area is titled 'Web Applications' and includes a search bar, a description, and a table of items. The table has columns for NAME, PRIVATE URL, CREATED DATE, and LAST MODIFIED. There are two items listed: 'Ping!' and 'YubiTest'. The 'Ping!' item has a launch icon (a blue square with a white play button) next to its name.

NAME	PRIVATE URL	CREATED DATE	LAST MODIFIED
Ping!	http://myDevBox2:3000	7/1/25, 10:03 AM	7/1/25, 10:03 AM
YubiTest	https://demo.yubico.com/webauthn	5/30/25, 4:47 PM	5/30/25, 4:47 PM

 **Note:** The session duration for the public URL is not the same as that for a platform portal session. Upon logging out of the platform portal, access to the public URL may remain available until the login token expires.



Note: While private web application sessions operate independently from Delinea Platform portal UI sessions, (i.e. logging out of the Platform does not terminate the Web Application session or require reauthentication) they adhere to the same refresh intervals and maximum session lengths as the browser session.

Public to Private URL Mapping

To better understand the way private URLs will be rendered, refer to the table below:

Example Web Application:

Private URL: `http://intranet:8080/finance/payments/index.html` mapped to

Public URL: `https://finance_payments-myco.go.delinea.app`

Launch Method	Browser URL	Shows Content From
Launching from the Inventory	<code>https://finance_payments-myco.go.delinea.app/finance/payments/index.html</code>	<code>http://intranet:8080/finance/payments/index.html</code>
Using a bookmark/manually going to the URL	<code>https://finance_payments-myco.go.delinea.app/finance/payments/index.html</code>	<code>http://intranet:8080/finance/payments/index.html</code>
	<code>https://finance_payments-myco.go.delinea.app/</code>	<code>http://intranet:8080/</code>
	<code>https://finance_payments-myco.go.delinea.app/some/other/path</code>	<code>http://intranet:8080/some/other/path</code>



Note: WebSockets are not supported.

Understanding PRA Permissions and Roles

The table below describes each permission available with PRA .

Permissions	Description	Permission List
Launch PRA Session	Launch a remote session. <i>Needed to use PRA .</i>	<code>delinea.platform/remotefaccess/session/launch</code>

Permissions	Description	Permission List
View Secrets	View the secrets in the Remote Access page. Applicable only for On-Prem Secret Server customers. <i>Needed to use PRA .</i>	delinea.platform/remotefaccess/secret/read
View PRA Engine	View the UI of a Remote Access engine.	delinea.platform/administration/remotefaccess/engine/read
Activate PRA Engine	Activate an engine to access and connect to your remote systems through a site and engine	delinea.platform/administration/remotefaccess/engine/activate
Add PRA Engine	Add an additional Remote Access engine to connect to remote systems.	delinea.platform/administration/remotefaccess/engine/create
Delete PRA Engine	Remove a Remote Access Engine from the server via automated uninstall or manually.	delinea.platform/administration/remotefaccess/engine/delete

Permissions	Description	Permission List
Update PRA Engine	Deploy the latest updates to your Remote Access engines.	delinea.platform/administration/remotearrress/engine/update
Create PRA Site	Create a new Remote Access site.	delinea.platform/administration/remotearrress/site/create
Delete PRA Site	Remove a Remote Access site.	delinea.platform/administration/remotearrress/site/delete
View PRA Site	View Remote Access site details.	delinea.platform/administration/remotearrress/site/read
Update PRA Site	Rename a Remote Access site.	delinea.platform/administration/remotearrress/site/update
Upload Files	This permission enables the user to upload a file to the target system during the remote access session.	delinea.platform/remotearrress/filetransfer/upload
Download Files	This permission enables the user to download a file from the target system during the remote access session.	delinea.platform/remotearrress/filetransfer/download

Permissions Applicable Only for Secret Server On-Premises

Permission	Description	Permission List
Add Secret Server On Premises Templates	Can add Secret Server On Premises templates	delinea.platform/administration/remotearchive/secrettemplate/create
Configure Secret Server On Premises integration	Can configure Secret Server On Premises integration	delinea.platform/administration/remotearchive/vault/configure
Delete Secret Server On Premises Templates	Can delete Secret Server On Premises templates	delinea.platform/administration/remotearchive/secrettemplate/delete
View Secret Server On Premises Templates	Can view Secret Server On Premises templates	delinea.platform/administration/remotearchive/secrettemplate/read
View Secret Server On Premises integration	Can view Secret Server On Premises integration	delinea.platform/administration/remotearchive/vault/read


RemoteApp Permissions |

Permission	Description	Permission List
Read Remote Applications	Can read remote applications	delinea.platform/remotearchive/remotearchive/read
Create Remote Applications	Can create remote applications	delinea.platform/remotearchive/remotearchive/create
Update Remote Applications	Can update remote applications	delinea.platform/remotearchive/remotearchive/update
Delete Remote Applications	Can delete remote applications	delinea.platform/remotearchive/remotearchive/delete

Web Application Permissions

Permission	Description	Permission List
Read Web Applications	Can read web applications	delinea.platform/remotearchive/webapplication/read
Create Web Application	Can create web application	delinea.platform/remotearchive/webapplication/create
Launch Web Application	Can a launch web application	delinea.platform/remotearchive/webapplication/launch
Update Web Application	Can update web application	delinea.platform/remotearchive/webapplication/update
Delete Web Application	Can delete web application	delinea.platform/remotearchive/webapplication/delete

Permissions From Other Delinea Platform Services

Permission	Description	Permission List
Secret Launch Remote Access (Platform)	<p>If your platform tenant does NOT have unified roles and permissions, then PRA users will need to be granted this permission in Secret Server. (Learn more).</p> <p> Important: Note that built-in RDP or SSH launchers must be enabled on a secret's template in Secret Server for the PRA launch link to be displayed.</p>	
View Site	Grants a user permission to read detailed information about a site.	delinea.enginepool/site/read

Permission	Description	Permission List
List Sites	View list of engine sites needed to allow users to select a site when connecting to a target machine.	delinea.enginepool/site/list
View Secret	To connect to PRA remote targets using vaulted credentials, ensure that this permission is enabled for all users. Additionally, users must have permissions for specific secrets.	delinea.vault/secretserver/secret/read

Hardening the PRA Engine Host



Important: This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

This topic discusses best practices for hardening Privileged Remote Access (PRA) engine servers.

PRA engines do not store any passwords, PII, or user data in any configuration files.

General Hardening Steps

Restrict Incoming Port Access to All PRA Engine Servers

PRA engines do not require any open incoming ports.

- Allow an SSH proxy port coming from the user's LAN.
- Block all other incoming ports.

Remove Unnecessary User Groups

For administrator user groups:

- Remove default domain admins, administrator and unused/unnecessary groups.
- Create one group that is going to have access to the PRA engine server(s)
- Disable the built-in local administrator user.

Rename Default Accounts

- Change the names of all administrator and guest accounts to names that do not indicate their permissions.
- Create a new locked and unprivileged "administrator" user name as bait.

Disable Services

Disable these services:

- None

Restrict Network Protocols

- None

SSL/TLS Settings

Keep your server SSL/TLS settings up to date. Among other settings, the different protocols and cipher suites can be vulnerable to different attacks on SSL/TLS.

- Disable SSL 2.0
- Disable SSL 3.0
- Disable TLS 1.0
- Disable TLS 1.1
- Enable TLS 1.2

System Admin - Universal



Important: This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

Network SSH/OpenSSL:

It is recommended to disable all network protocols not in use.

It is recommended that the operating system configures the uncomplicated firewall to rate-limit impacted network interfaces.

It is recommended that the operating system has an application firewall installed in order to control remote access methods.

It is recommended that customers use host-based endpoint protection (which includes FIM, firewall, anti-malware, alerting and monitoring, etc.)

It is recommended that the operating system immediately terminates all network connections associated with SSH traffic after a period of inactivity.

Privileged Remote Access

It is recommended that the operating system uses SSH to protect the confidentiality and integrity of transmitted information.

It is recommended that the operating system configures the SSH daemon to use Message Authentication Codes (MACs) employing FIPS 140-2 approved cryptographic hashes to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.

- It is recommended that SSH root login is disabled
- It is recommended that SSH HostbasedAuthentication is disabled
- It is recommended that SSH PermitEmptyPasswords is disabled
- It is recommended that SSH PermitUserEnvironment is disabled
- It is recommended that SSH IgnoreRhosts is enabled
- It is recommended that SSH X11 forwarding is disabled
- It is recommended that only strong ciphers are used
- It is recommended that SSH AllowTcpForwarding is disabled
- It is recommended that SSH MaxAuthTries is set to 4 or less
- It is recommended that SSH MaxStartups is configured
- It is recommended to set SSH MaxSessions to the minimum value needed by system administrators to manage the host machine
- It is recommended that SSH LoginGraceTime is set to one minute or less
- It is recommended that SSH Idle Timeout Interval is configured
- It is recommended that sudo commands use `pty`

Auditing

It is recommended that the operating system configures audit tools to be owned by root, group-owned by root with a mode of 0755 or less permissive.

It is recommended that the operating system is configured so that audit configuration files are not write-accessible by unauthorized users.

It is recommended that the operating system is configured so that the audit log directory is not write-accessible by unauthorized users.

It is recommended that the operating system permits only authorized groups ownership of the audit log files.

It is recommended that the operating system is configured to permit only authorized users ownership of the audit log files.

It is recommended that the operating system is configured so that audit log files are not read or write-accessible by unauthorized users.

It is recommended that the operating system generates audit records when successful/unsuccessful attempts to use the following commands:

Privileged Remote Access

- fdisk
- modprobe
- usermod
- gpasswd
- passwd
- sudo
- sudoedit/visudo
- umount
- mount
- su


CIS standards

- It is recommended that the mounting of cramfs filesystems is disabled
- It is recommended that the mounting of squashfs filesystems is disabled
- It is recommended that the mounting of udf filesystems is disabled
- It is recommended that the nodev option set on /var partition
- It is recommended that the nodev option set on /var/tmp partition
- It is recommended that the nodev option set on /var/log partition
- It is recommended that the noexec option set on /var/log partition
- It is recommended that the noexec option set on /var/log/audit partition
- It is recommended that the nodev option set on /var/log/audit partition
- It is recommended to disable Automounting
- It is recommended to disable USB Storage

If SNMP is installed, it is recommended to use a complex community string.:

- It is recommended that packet redirect sending is disabled
 - It is recommended that IP forwarding is disabled
 - It is recommended that ICMP redirects are not accepted
 - It is recommended that broadcast ICMP requests are ignored
 - It is recommended that bogus ICMP responses are ignored
 - It is recommended that IPv6 router advertisements are not accepted
-

Ubuntu

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

The following are Delinea recommended best practices for hardening the Ubuntu Linux distribution running the PRA engine. Customers are responsible for managing their own servers.

System Ubuntu:

It is recommended that the Ubuntu operating system immediately notifies the SA and ISSO (at a minimum) when the allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity.

It is recommended that the Ubuntu operating system prevents direct login into the root account.

It is recommended that the Ubuntu operating system ensures only users who need access to security functions are part of sudo group.

It is recommended that the Ubuntu operating system encrypts all stored passwords with a FIPS 140-2 approved cryptographic hashing algorithm.

It is recommended that the Ubuntu operating system prevents all software from executing at higher privilege levels than users executing the software and the audit system is configured to audit the execution of privileged functions.

It is recommended that the operating system automatically terminates a user session after inactivity timeouts have expired.

It is recommended that Ubuntu operating systems, when booted, require authentication upon booting into single-user and maintenance modes.

It is recommended that the operating system records time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).

(Setting limits file in /etc/security/limits.conf) It is recommended that the operating system limits the number of concurrent sessions to ten for all accounts and/or account types.

It is recommended that the Ubuntu operating system not have the telnet package installed.

It is recommended that the Ubuntu operating system is configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in their vulnerability assessments.

It is recommended that the Ubuntu operating system is configured to use [TCP syncookies](#).

It is recommended that the Ubuntu operating system disables kernel core dumps so that it can fail to a secure state if system initialization fails, shutdown fails or aborts fail.

It is recommended that the Ubuntu operating system deploys Endpoint Security for Linux Threat Prevention (ENSLTP).

It is recommended that the Ubuntu operating system is configured to preserve log records from failure events.

It is recommended that the Ubuntu operating system synchronizes internal information system clocks to the authoritative time source when the time difference is greater than one second.

Privileged Remote Access

It is recommended that the Ubuntu operating system's Advance Package Tool (APT) is configured to prevent the installation of patches, service packs, device drivers, or Ubuntu operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization.

It is recommended that the Ubuntu operating system is configured to use a Linux Security Module implementation of name-based mandatory access controls.

It is recommended that the Ubuntu operating system implements address space layout randomization to protect its memory from unauthorized code execution.

It is recommended that the Ubuntu operating system, for networked systems, compares internal information system clocks at least every 24 hours with a server which is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, and/or the Global Positioning System (GPS).

Directories, Files and Permissions

It is recommended that the /var/log directory is owned by root, group-owned by syslog and have mode "0755" or less permissive.

It is recommended that the /var/log/syslog file is owned by syslog, group-owned by adm and have mode 0640 or less permissive.

It is recommended that directories that contain system commands are owned by root, group-owned by root set to a mode of 0755 or less permissive.

It is recommended that the Ubuntu operating system library directories and files are owned by root, group-owned by root or a system account set to a mode of 0755 or less permissive.

Red Hat Enterprise Linux - RHEL



Important: This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

The following are Delinea recommended best practices for hardening the RHEL distribution running the PRA engine. Customers are responsible for managing their own servers.

System RHEL:

It is recommended that RHEL be a vendor-supported release.

It is recommended that vendor packaged system security patches and updates are installed and up to date.

It is recommended that the rsyslog service is running in RHEL.

For RHEL systems using Domain Name Servers (DNS) resolution, it is recommended that at least two name servers are configured.

It is recommended that RHEL is securely compared to internal information system clocks at least every 24 hours with a server synchronized to an authoritative time source, such as the United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DoD network, and/or the Global Positioning System (GPS).

Privileged Remote Access

It is recommended that RHEL does not have the telnet-server package installed.

It is recommended that RHEL enables mitigations against processor-based vulnerabilities.

Directories, Files and Permissions:

It is recommended that the /var/log Directory is owned by root, group-owned by root and have mode 0755 or less permissive

It is recommended that the /var/log/messages File is owned by root, group-owned by root and have mode 0640 or less permissive

It is recommended that system commands are owned by root, group-owned by root (or a system account) and must have mode 0755 or less permissive.

It is recommended that library directories are owned by root.

It is recommended that SSH private host key files are mode 0640 or less permissive.

It is recommended that RHEL restricts privilege elevation to authorized personnel.

It is recommended that RHEL prevents the installation of software, patches, service packs, device drivers, or operating system components from a repository without verification they have been digitally signed using a certificate that is issued by a Certificate Authority (CA) that is recognized and approved by the organization.

Network SSH/OpenSSL:

It is recommended that a firewall is active on RHEL.

It is recommended that an RHEL firewall employs a deny-all, allow-by-exception policy for allowing connections to other systems.

It is recommended that RHEL ignores and/or prevents IPv6 Internet Control Message Protocol (ICMP) redirect messages from being accepted.

It is recommended that the RHEL operating system implements a DoD-approved encryption to protect the confidentiality of SSH server connections. The RHEL operating system must implement DoD-approved encryption in the OpenSSL package. RHEL must ensure the SSH server uses strong entropy.

Understanding PRA Entitlements

PRA concurrent user licenses entitle users on that tenant to connect to remote systems using PRA . Each concurrent user license is consumed by one user when they start their first remote connection. Each user is entitled to a maximum of 4 concurrent remote sessions. The license continues to be in use by that user for the total duration of all their concurrent remote sessions until their last remote session ends. At this time the license is released for use by other users.

Additionally, each PRA concurrent user license also entitles users to limited capabilities in Secret Server (shown in the Vendor User column in the link below) and no additional Secret Server licenses are needed to exercise these capabilities. The Platform user membership-type is used to manage these entitlements. Learn more about managing Secret Server entitlements for 3rd party users in ["Contractor and Vendor Access" on page 519](#).

Please note that PRA concurrent licenses are consumed as outlined in the first paragraph, regardless of whether a user has Vendor User entitlements or IT User entitlements in Secret Server.

Understanding PRA Workloads on the Delinea Platform Engine

PRA workloads are now available on Windows and Linux environments. Please see [Privileged Remote Access Workload](#) for more information.

PRA Troubleshooting

This section provides helpful troubleshooting tips and answers to frequently asked questions.

- "Failed to Connect to the Target Machine" below
- "The Engine is Configured Properly But a Connection to the Target Cannot Be Established" on the next page
- "Unable to Launch SSH Sessions via Secret Server Distributed Engine" on page 360
- "Issues Connecting to On-Prem Secret Server" on page 361

Failed to Connect to the Target Machine

Failed to Connect to the Target Machine. Error Showing When Attempting to Launch a Remote Session. The cause of this problem could be that the user's engine server was not properly configured to use the DNS for their environment. The engine may be unable to resolve the DNS name for the selected target.

To fix this problem:


- Check that the correct site was selected in the site selection dialog drop-down menu.
- Check that the target server is up and running
- Ensure that the target server is routable from the engine server (e.g. 192.168.x.x engine server will need routes correctly set up to connect to a 10.10.x.x target server)
- Verify the secret data is correct (URL(Machine), Password, Public Key, Private Key, Private Key Passphrase)
- Check that the proper Secret template was used
- Check that secret "Approval" was granted if necessary and that all security requirements are satisfied.
- Do ensure that the engine for the site you selected is "Online" (the engine may have gone offline close to the time the user selected the site to connect to)

RDP Supported Authentication Methods

PRA currently supports Enhanced RDP Security with TLS Encryption and NTLM authentication (CredSSP). The target machine needs to have NLA enabled and NTLM authentication traffic needs to be enabled. [Standard RDP Security](#) is not currently supported.

Kerberos authentication is supported. See "Kerberos Authentication" on page 298 to learn more.

The Engine is Configured Properly But a Connection to the Target Cannot Be Established

 **Note:** This section requires root access to the target server and assumes the target server has a recent version of OpenSSH/OpenSSL installed, configured correctly and running successfully.

1. OpenSSH information:

- PRA supports versions OpenSSH_7.4p1, OpenSSL 1.0.2k-fips and up to version OpenSSH_8.x, OpenSSL 1.1.1k.
- The newest version of OpenSSH is 9.x. This version may function but is not yet fully supported.
- Older versions may still function but are not supported.

2. Verify the configuration on the target server:

- SSH into the Linux target server.

```
ssh user@targetServer [-i /path/to/pubkey]
```

- Sudo into root
 - Some Linux distributions require superuser privileges to run the following commands
- Run the following command to verify SSH is installed and is a supported version:

```
ssh -V
```

- Run the following command to verify SSHD is running and listening for incoming connection requests:

```
netstat -plnt
```

- Look for sshd in the output of the above command in the column titled PID/Program name.

```
[ec2-user@ip-10-200-21-138 ~]$ sudo netstat -plnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1020/sshd
tcp6       0      0 :::22                   :::*                     LISTEN      1020/sshd
tcp6       0      0 :::80                   :::*                     LISTEN      91881/clientmgr
```

- Check the Local Address column for SSHD and verify it is listening on port 22 i.e. 0.0.0.0:22

```
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1020/sshd
```

Accessing Logs on the Engine Server

The following command(s) will display a real time update to the users screen containing "Login" logs for the server. Type control c (^c) (hold down the "control" key then type the letter c) to exit the command on any operating system.

Privileged Remote Access

- Debian/Ubuntu

```
tail -f /var/log/auth.log
```

- RHEL/Redhat 7 & 8/Amazon

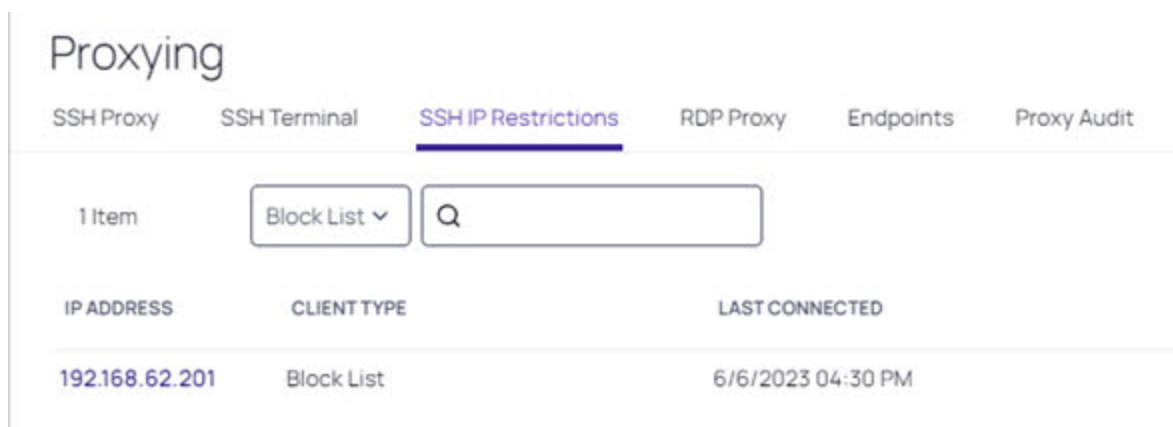
```
tail -f /var/log/secure
```

1. Check if the users request is getting to the target server.
 - Run the command above
 - From the web UI select the secret for the target server you are logged into.
 - From the SSH shell check the logs:
 - Is the request showing up in the logs? If not then check the "Machine" data in the secret is correct.
 2. Check if the users request is being rejected:
 - Run the command above
 - From the web UI select the secret for the target server you are logged into.
 - From the SSH shell check the logs:
 - Does the log entry contain an error e.g. "Invalid user ", "Incorrect password" or "Invalid public key"? If so check the secret data and confirm the password, private/public key or key passphrase is correct.
-

Unable to Launch SSH Sessions via Secret Server Distributed Engine

Possible solutions:

1. Check your SSH IP restrictions inside the Delinea Platform to make sure there are no Secret Server IP restrictions preventing the SSH sessions from launching.



2. Enable debug mode in the distributed engine. Please review the [Secret Server documentation](#) for more information.

Privileged Remote Access

- Turn off the **Enable Block Listing** setting. This will prevent incoming IP addresses from being blocked if a user fails to authenticate in the maximum number of attempts.

Admin >

Proxying

SSH Proxy SSH Terminal SSH IP Restrictions RDP Proxy Endpoints Proxy Audit

Proxy New Secrets By Default	Yes	Edit
Enable SSH Proxy Inactivity Timeout	No	Edit
SSH Proxy Banner	=== Welcome to the Secret Server SSH Proxy ===	Edit
Hide passwords from SSH keystroke capture	No	Edit
Send window title change command on startup	No	Edit
SSH Proxy Host Fingerprint	MD5 - 51:51:cb:cf:9f:6f:c5:a3:ee:b1:15:29:b3:58:4a:ff SHA1 - 0f:ae:78:75:3d:82:e7:91:74:f4:19:65:6e:d0:9a:cf:e5:d3:47 SHA256: A22n6pxDPL2w1FLJ25gozoG0uxV0Hb7Yd03gwT6h9no SHA512: bV7Q8Q6ctp+23Yy20FE6QJTGkH1cKhtYU7s5uEEJAabud5QL8U5+mbRanKYh10z2P73DP91sHcwc5ewj5hD/Yig	Edit Generate ECDSA RSA

SSH Proxy Block List Settings

- SSH Proxy can block incoming clients that connect and fail to authenticate.

Enable Block Listing	Yes	Edit
Auto Block Max Attempts	5	Edit
Auto Block Max History	100	Edit
Auto Block Time Frame (minutes)	30	Edit

Client Override IP Address Ranges

Add

- Specific IP address ranges can be configured to always allow or always block the incoming connection



Note: The Auto Block Max Attempts is set to 5 attempts by default. This can be raised or lowered as needed.

Issues Connecting to On-Prem Secret Server

If the PRA engine cannot connect to the target on-prem Secret Server, check if the on-prem Secret Server is accessible from the PRA engine by running the following commands:

```
curl -kv https://ON PREM SECRET SERVER DOMAIN NAME or IP ADDRESS/api/v1/users/current
```

Troubleshooting Connection Issues Between Secret Server On-Premises and the Delinea Platform

If you are seeing a "Not Connected" error message in the platform UI, try the following troubleshooting steps:

- Navigate to the Delinea Platform integration configuration.
 - Check the values (Platform URL, etc.)
 - See if you can search for and find a new Platform group to add
 - See if you can run a synchronize operation against Platform
- If the actions in Step 1 work, then the Client ID/Secret for the Platform are correct. At that point, proceed to checking the individual users for which you are trying to use PRA.

- a. Are they active?
 - b. Do they have the Platform permission to use PRA?
 - c. Does the tbPlatformPermissionCache table for those users hold the Platform permissions that PRA requires?
-

The Engine Shows as "Offline"



Important: This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

The Engine Shows as "Offline" in the Engine Management UI

Possible solutions:

1. Check that the engine has been activated. To activate an engine, open the site that contains the engine and then choose "Activate" from the context menu on the row containing the engine.
 - Check that the engine server is active. Create a direct SSH connection to the engine server and run the following command:

```
sudo systemctl status clientmgr
```

- Ensure that the **Status** is *Active*:

```
Active: active (running) since Tue 2022-11-29 19:44:19 UTC; 8s ago
```

- The above command also prints the latest engine logs. Check the output for any clear errors such as:

```
Process: 53415 ExecStart=/usr/local/bin/clientmgr (code=exited, status=1/FAILURE)
```

2. Check for any clear errors by running the following command (internal only):

```
journalctl -u clientmgr -r
```

- Check the printed output for any clear errors, such as the following:

```
Nov 29 19:57:11 ip-10-200-21-138.eu-west-1.compute.internal clientmgr[53431]: Post  
"https://tenant.ras-tunnels.delinea.app/registrar/registration": remote error: tls:  
unrecogniz>
```


3. Check the Engine Update Version:

- Any engine version 0.0.23 or lower must be [manually deleted](#) and a new installation must occur to update to the latest version.
- Verify the UI engine record has been *Deleted* from the *Site*. See the following [online help page](#) for more information.

Unable to Open an SSH Session From the Web UI

Use telnet or netcat to connect to the target server from the engine server on port 3389. Being unable to connect to the target server may indicate that the problem is occurring on the target server. The same command may also be used to debug SSH problems by connecting to the target server on port 22 (or whichever port on the target is hosting the SSH daemon).

- `telnet <tar.get.ip.here> 22`
- `netcat <tar.get.ip.here> 3389` OR `nc <tar.get.ip.here> 3389`

Unable to Open an RDP Session From the Web UI

Telnet into target server from the engine server on port 3389. Being unable to telnet into the target server indicates an issue is occurring on the target server.

```
telnet <tar.get.ip.here> 3389
```

Engine Seems to be Functioning in an Unexpected Manner

1. Check that the server resources are available and not overloaded
2. Check available disk/storage space

```
df -h
```

```
[ec2-user@ip-10-200-21-138 ~]$ df -h
Filesystem      Size  Used Avail Use% Mounted on
devtmpfs        854M   0  854M   0% /dev
tmpfs           888M  12K  888M   1% /dev/shm
tmpfs           888M  50M  838M   6% /run
tmpfs           888M   0  888M   0% /sys/fs/cgroup
/dev/nvme0n1p2  10G   10G   28M 100% /
/dev/loop0       50M   50M   0 100% /var/lib/napd/snap/snapd/17883
/dev/loop1       64M   64M   0 100% /var/lib/napd/snap/core20/1695
/dev/loop2       6.7M  6.7M   0 100% /var/lib/napd/snap/links/60
/dev/loop3       64M   64M   0 100% /var/lib/napd/snap/core20/1738
tmpfs           178M   0  178M   0% /run/user/1000
```

3. Check that memory is available and not "swapping"

```
free -m
```

```
[ec2-user@ip-10-200-21-138 ~]$ free -m
              total        used        free      shared  buff/cache   available
Mem:           1774          311          420           50        1042        1230
Swap:            0            0            0
```

4. Check that CPU is not overloaded (check the %Cpu row, item = id/idle)

```
top
```

```
top - 01:36:07 up 31 days, 4:41, 2 users, load average: 0.00, 0.00, 0.00
Tasks: 103 total, 1 running, 102 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.2 us, 0.0 sy, 0.0 ni, 99.8 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 1774.6 total, 419.0 free, 312.6 used, 1042.9 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used. 1229.4 avail Mem
```

Setting a Static UUID

UUIDs need to persist between reboots. If you are using any virtualized infrastructure where UUIDs are changing, please make sure to keep the UUID stable.

Setting a Static UUID in Skytap

Before creating a static UUID, check to see if the engine is offline by running the following command:

```
sudo systemctl status clientmgr.service
```

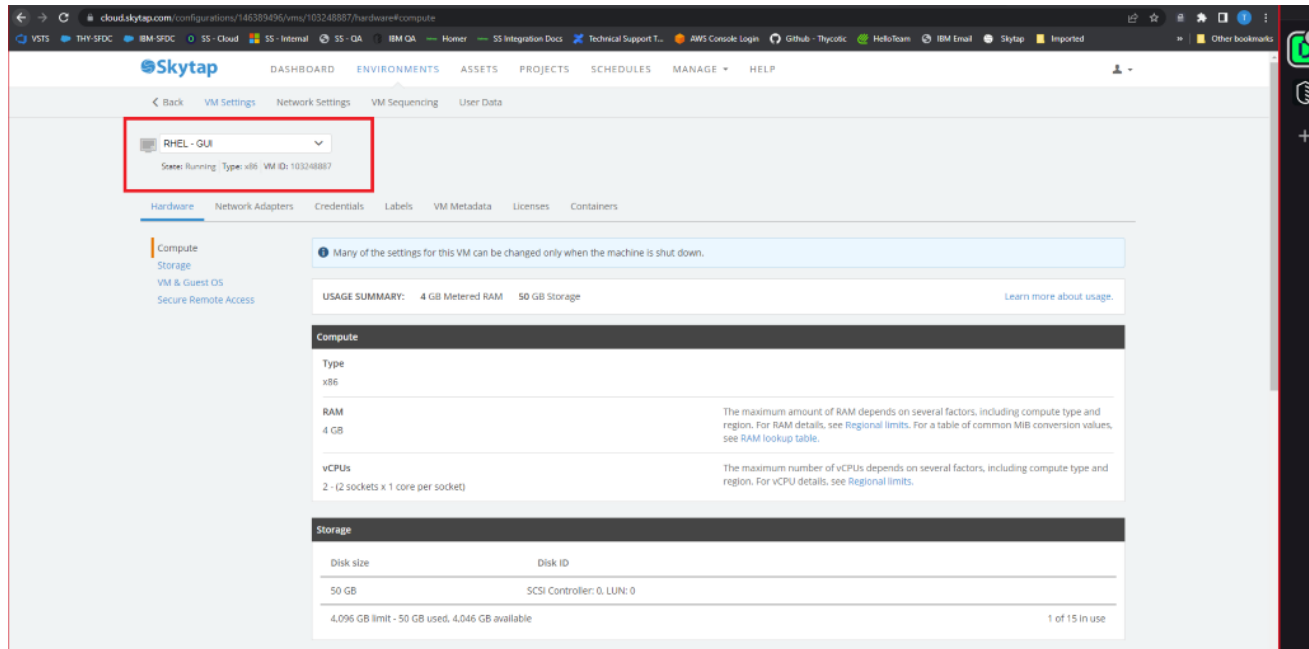
If the web UI shows the engine is offline, proceed to creating a static UUID:

Privileged Remote Access


1. SSH into the server with the following command:

```
sudo cat /sys/devices/virtual/dmi/id/product_uuid
```




2. In Skytap > Navigate to the **Environment Page > VM Settings**
3. Select the name of the Linux VM from the drop-down.



4. Copy and paste the UUID into the web UI.


 **Note:** The VM needs to be stopped prior to entering the UUID in the web UI.

Privileged Remote Access

VM & Guest OS	
Hardware version 11	Make sure the VM is using the latest version of VMware Tools for Linux or Windows before you upgrade. You can save this environment as a template before you upgrade so that you can roll back your changes if something get wrong.
Guest OS Red Hat Enterprise Linux 7 (64-bit) 	Setting the Guest OS determines available hardware for the VM. Learn more.
Boot mode <div>BIOS </div>	Change this setting to enable UEFI VM imports to boot. Changing the boot mode of a working VM may prevent the VM from starting. Learn more.
Nested virtualization <input type="checkbox"/> Enable nested virtualization	Nested virtualization lets you run a virtual machine inside of a virtual machine. For more information, including a list of operating systems that support this feature, see Enabling nested virtualization .
Time sync Automatic 	To sync the BIOS clock with the current date and time every time you run the VM. Learn more.
Custom UUID <div>42354D61-A66E-E83C-0CF8-F26A43D3357F</div>	A universally unique identifier is generated using a timestamp. UUID has a maximum of 32 hexadecimal characters (0-9, A-F, a-f). Learn more.
<div>Save Cancel</div>	

5. Save the web form and start the server.
6. Run the same terminal commands in the Linux machine to verify it's the same.
7. Install the PRA engine

Issues Installing the PRA Engine

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309

If users encounter issues during PRA installation, check to make sure your Linux distribution is supported:

- Amazon Linux 2, Amazon Linux 2023+
- Debian 8.x+
- Ubuntu 18.x+
- Redhat 7.x + (Will be deprecated by the end of 2024. Only Redhat 8+ will be supported going forward)

We also recommend that users have:

- At least 1 GB of physical RAM
- At least 500 MB storage

Warnings That Can Occur During Installation

1. Unsupported operating system
 - **Warning msg:** "This Linux distribution or version is NOT currently supported!"
2. Unsupported operating system "Version"
 - **Warning msg:** "Unsupported system version OS 6.3, required 7"
3. Not enough physical memory
 - **Warning msg:** "This system has less than 1Gb, of available memory! Performance may be degraded."
4. Not enough physical storage
 - **Warning msg:** "Not enough space on disk 250mgb, required 1 GB"
5. Non-unique engine name
 - **Warning msg:** "The engine name "" is already in use for this site. Please enter a unique engine name."

Errors That Can Occur During Installation:

1. User does not have root/privileged/administrator access
 - **Error msg:** "Super user privileges are required to install PRA ."
 - **Solution:** User must have root access to run the installer
2. A previously installed version of the PRA engine has been detected
 - **Error msg:** "A previously installed version of PRA has been detected."
 - **Solution:** User must un-install the currently installed PRA engine
3. Installation script has expired
 - **Error msg:** "This installation script has expired."
 - **Solution:** User must return to the web UI and generate a new installer script
4. Unable to finalize installation
 - **Error msg:** "Unable to finalize installation with PRA registration service"
 - **Solution:**
 - a. Check that only one user is installing using the engine name they entered. (if 2 users try to install on different servers at the same time and enter the same engine name the registration will be rejected)
5. The engine host cannot be uniquely identified
 - **Error msg:** Unable to retrieve this device's unique identifier.
 - **Troubleshooting:**
 - Run the following command:
`sudo cat /sys/devices/virtual/dmi/id/product_uuid`
 - Check if the following error appears: *No such file or directory*

■ **Solution:**

- This issue can occur if installing the engine in a container, which is unsupported.
- This issue can also occur if the server configuration does not include this file, which is needed to uniquely identify a PRA engine. Please install the PRA engine on a host that is configured to ensure that this file exists.

6. Failure while running the installer on Ubuntu hosts

- **Error msg:** "chmod: cannot access '/tmp/installer': No such file or directory"
- **Solution** This error may appear if curl was installed with *snap* instead of *curl*. Please uninstall the curl package using *sudo snap remove curl* and reinstall it with *sudo apt install curl*.

7. Server registration error

- **Error msg:** This server is currently registered with another site.
- **Solution:**
 - a. Have the user check that this server has been deleted from the web UI. (If this server has had a previous PRA installation that was manually deleted and the Web UI record was NOT deleted, this error will occur).
 - b. Check that this server has not been previously registered with a different tenant.

8. The engine cannot be identified and registered in the Delinea Platform

- **Error msg:** Registration error
- **Solution:**
 - a. This happens when the *product_uuid* of the Linux system was changed.
 - Check if the *product_uuid* was changed after restart:

```
cat /sys/devices/virtual/dmi/id/product_uuid
```

- Reinstall the engine

Uninstallation of the PRA Engine is Not Working From the Web UI.

1. SSH into the server hosting the PRA engine
2. Run the following CLI command as a privileged user:


```
- sudo /opt/delinea/updater -del
```



Note: If the command above did not work as expected, please try the following commands:


- `systemctl stop clientmgr`
- `rm -f /etc/systemd/system/clientmgr.service`
- `rm -rf /etc/clientmgr`

- `rm -f /usr/local/bin/clientmgr`
- `rm -f /usr/local/bin/tunnelcl`
- `rm -f /usr/local/bin/updater`
- `rm -rf /opt/delinea`
- `systemctl daemon-reload`

 **Important:** Please use with caution. This is a hard reset

3. To uninstall PRA engines from the Web UI, see [Uninstall PRA Engines](#).

Using Start/Stop Commands

 **Important:** This content applies to the deprecated standalone Delinea PRA Engine. Existing PRA Engines will continue to operate normally but customers can no longer create new PRA Engines or Sites. For all new deployments, use the Platform Engine with the [PRA Workload](#). To upgrade previously deployed PRA Engines, see "Upgrading Standalone PRA Engine to the Delinea Platform Engine" on page 309


The following Start and Stop commands can be run if issues are encountered and are not resolved by other troubleshooting solutions:

- To manually stop the PRA engine:

```
sudo systemctl stop clientmgr.service; echo $?
```

- To manually start the PRA engine:

```
sudo systemctl start clientmgr.service; echo $?
```

 **Note:** Look for the 0 to verify that the commands were successful. Any other value indicates a failure

SAML and OIDC Federation

Federated identity management is a method for using a single user identity in multiple different identity management systems. In Delinea Platform, Federation enables users to log on using credentials from a trusted third-party federated identity provider (IdP). When a user initiates login, the platform checks the domain name of the user ID. If the domain is configured for an external federated IdP, the login data is passed to that provider, and the user is authenticated and logged in.

The Delinea Platform currently supports two authentication protocols:

- Open ID Connect (OIDC)
- Security Assertion Markup Language (SAML)



Note: You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

Multiple federated identity providers can be configured on the platform, based on your specific needs and the supported protocols by the identity provider (IDP).

Platform Federation Integrations

The Delinea Platform integrates with numerous Single Sign-On (SSO) identity providers. The configuration articles below cover some of the most common ones. If your preferred IdP isn't listed, for example DUO, you can still configure it using your official IdP provider documentation and the information provided here.

- [Integrating AD FS](#)
- ["Integrating Auth0" on page 390](#)
- [Integrating BlokSec](#)
- [Integrating Celestix](#)
- ["Integrating Entra ID" on page 397](#)
- ["Integrating Entrust" on page 415](#)
- [Integrating Google](#)
- ["Integrating Okta" on page 437](#)
- ["Integrating OneLogin" on page 447](#)
- ["Integrating Ping Identity" on page 457](#)
- [Integrating RSA](#)



Note: Instead of using [Integrating Entra ID](#) federation, you can use Entra ID as a Registered App (native integration). See [API-Based Integration with Entra ID](#). But you cannot use both Entra ID features simultaneously with the same domains.

Supported SSO Approaches

SSO simplifies user access across multiple applications with a unified login. The Delinea Platform supports two approaches:

- SP-initiated SSO
- IdP-initiated SSO

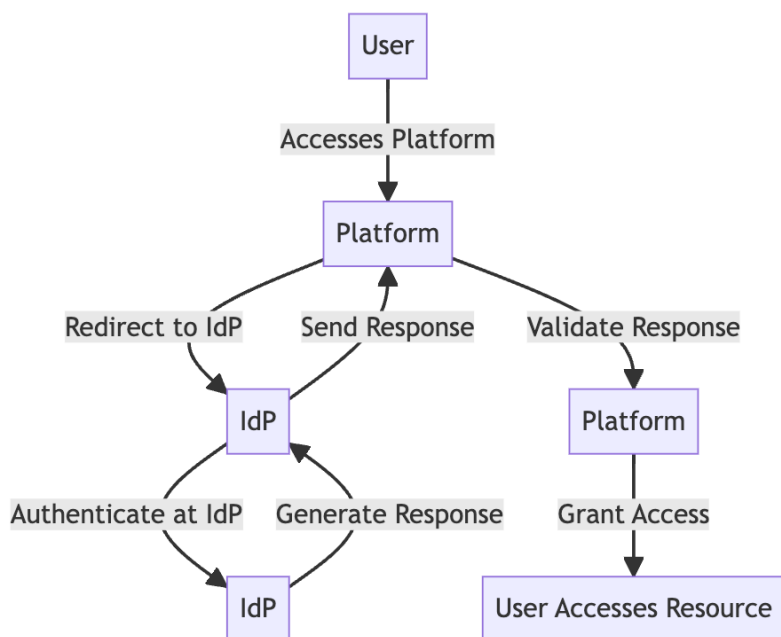
Each approach serves specific organizational needs and identity and access management (IAM) architectures.

Feature	SP-initiated SSO	IdP-initiated SSO
Initiation of authentication flow	Service provider	Identity provider (IdP)
User logs in to	Delinea Platform	IdP portal, such as MyApps for Microsoft
User experience	User is redirected from the Delinea Platform to the IdP for authentication; when granted, the user is returned to the platform	User selects the Delinea Platform from among the apps on the IdP site
Organizational needs	Environments where customers are offered direct access to the Delinea Platform	Environments where multiple applications are offered

SP-Initiated SSO

SP-Initiated SSO starts the initiation of the authentication flow at the Service Provider (SP). In this scenario, a user's interaction with the Delinea Platform (SP) triggers the need for authentication.

The diagram below depicts the sequence of actions in SP-initiated SSO at a high level. The specific steps of these flows may vary depending on the chosen SSO protocol, such as SAML or OpenID Connect.

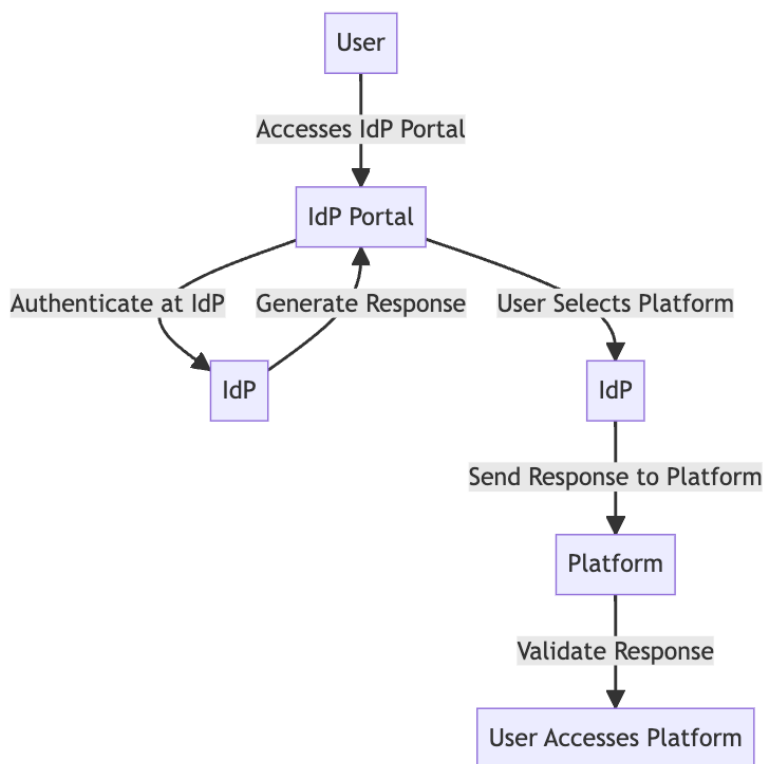


1. The user starts by accessing the Delinea Platform (SP in this case).
2. The platform redirects the user to the Identity Provider (IdP) for authentication.
3. The user authenticates at the IdP.
4. The IdP creates an authentication response.
5. This response is then transmitted from the IdP to the platform.
6. The Delinea Platform validates the response and grants the user access.

IDP-Initiated SSO

IDP-Initiated SSO follows a different initiation model. Here, the authentication flow starts at the Identity Provider (IdP). Users typically log in at the IdP's portal, such as MyApps for Microsoft, where they are authenticated. After successful authentication, the IdP provides the user with a list of available applications they can access without needing to re-enter their credentials.

The diagram below depicts the sequence of actions in IdP-initiated SSO at a high level. The specific steps of these flows may vary depending on the chosen SSO protocol and technology, such as SAML or OpenID Connect.



1. The user starts by accessing the IdP's portal.
2. The user authenticates at the IdP.
3. The IdP generates an authentication response.
4. The IdP presents a list of applications (Delinea Platform is one of them).

5. The user selects the Delinea Platform application.
6. The IdP sends the response to the selected Service Provider (SP).
7. The platform validates the response and then grants the user access to log in.

For related content, see the following:

- [Federation Management](#)
- [Troubleshooting Federated Group Mapping](#)

Managing Federations

Add a Federation Service Provider

1. From the left navigation, click **Settings**, then select **Federation providers** from the secondary menu.
2. On the Federation Providers page, click the **Add Provider** button.
3. Select SAML or OIDC. The Add Provider page opens, displaying all controls necessary for adding a provider.



Note: You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

Consult the detailed documentation for these specific IdPs:

- [Integrating AD FS](#)
- "Integrating Auth0" on page 390
- [Integrating BlokSec](#)
- [Integrating Celestix](#)
- "Integrating Entra ID" on page 397
- "Integrating Entrust" on page 415
- [Integrating Google](#)
- "Integrating Okta" on page 437
- "Integrating OneLogin" on page 447
- "Integrating Ping Identity" on page 457
- [Integrating RSA](#)



Note: Refer to your IdP's documentation for guidance on SSO integration, as similar procedures can be followed for the Delinea Platform.

Enable a Federation Service Provider

1. From the left navigation, click **Settings**, then select **Federation providers**.
2. Click the name of one of the federation providers listed.
3. On the Settings tab, click **Edit**.

4. Next to Status, select the Enable check box.
5. Click **Save**.

Delete a Federation Service Provider

1. From the left navigation, click **Settings**, then select **Federation providers**.
2. Click the name of one of the federation provider you wish to remove.
3. Delete the provider from either the table, the preview panel, or the provider's detail page.



Note: You cannot delete a provider when it is in an enabled state, so you must disable the provider prior to deleting it. Proceed with caution when deleting the provider, as this action may affect user access to the platform, and it cannot be undone.

Advanced Settings (SAML only)

Advanced Settings

Customize certificate issuer sent to IdP	<input type="checkbox"/>
Force Authentication (ForceAuthN)	<input type="checkbox"/>
Use Login Hint	<input type="checkbox"/>
Request binding	<input type="text" value="HTTP-Redirect"/>
Sign Request	<input type="checkbox"/>

Customize Certificate Issuer Sent to IdP: This setting overrides the default Certificate Issuer information sent by the platform to the Identity Provider (IdP). This setting should be used cautiously and only when necessary to maintain compatibility with your IdP configuration.

ForceAuthN: Select the checkbox to force authentication, or deselect it to disable forced authentication. When enabled, the Force Authentication (ForceAuthN) setting asks the identity provider (IdP) to require the user to authenticate again, even if the user has an existing session or has previously authenticated. The IdP must ignore any existing session and prompt the user to provide their credentials for authentication. The support and behavior for this option may vary depending on the IdP's SAML implementation.

Use Login Hint: This setting applies to SAML. Enabling this option transmits the username to the IdP using the login_hint parameter in the HTTP request, with the username automatically populating during the login process to the IdP. For OIDC, the username is always passed to the IdP. Please refer to your IdP documentation to confirm whether this configuration is supported and to understand its implementation details.

Request Binding: This setting controls the method for binding SAML authentication requests to the communication protocol. By default, it is set to 'HTTP-Redirect' for URL-based binding but alternatively can be set to 'HTTP-POST' for form-based binding.

Sign Request: When enabled, this setting ensures that the SAML authentication request sent to the identity provider is digitally signed for added security. You can upload the certificate in either format pfx or p12.

Advanced Settings (OIDC only)

Platform federation functionality supports two OIDC flows: Code Flow and Implicit Flow.



Note: For optimal security and reliability, Delinea recommends using **Code Flow** by default. **Implicit Flow**

Advanced Settings

Enable Implicit Flow ☐ No ☐

Code Flow (Default):

- Applied by default
- Includes an additional step where an authorization code is exchanged for tokens
- Strongly recommended due to its superior security features, and suitable for most scenarios

Implicit Flow (Optional):

- Allows clients to directly obtain ID Tokens after authentication
- Not recommended due to its inherent security vulnerabilities

Re-authentication with the IdP

By default, federated users are not prompted to re-authenticate with the IdP every time they try to log in to the platform, assuming the user has a valid authentication session with the IdP. This experience may not be desired on shared workstations, or if re-authentication is required for sensitive operations, such as managing requirements for governance. The platform allows Administrators to configure the desired behavior as needed for SAML or OIDC providers. When the user logs out of the Delinea Platform, the user's overall session with the IdP is not impacted or invalidated.

Prompt for Re-authentication (OIDC only)

1. On the IdP provider's page, click **Edit**.
2. Under **Settings**, set **Prompt** to the desired option.

Support for these options depends on the OIDC implementation used by the IdP.

Option	Description
Not specified	Default option. If the user has a valid authentication session with their IdP, they will not be prompted to authenticate again. If the user is not authenticated or has no active session, they will be redirected to the IdP to initiate the authentication process.

Option	Description
Prompt for Authentication (login)	Every time the user logs out of the platform and tries to log back in, they will be required to enter their credentials and authenticate with their IdP again, even if they are already logged in.
Select Account (select_account)	This option forces the user to select an account to authenticate with. This is useful when you want to provide the user with the option to switch accounts.

Attribute Mappings

User attributes are passed from an identity provider (IdP) such as Auth0 to the Delinea Platform Service Provider (SP) during the authentication and authorization process. Some default attributes for SAML and OIDC are provided by default, and new, custom attributes can be added.

The following screen shot provides an example set of custom attributes for SAML with Auth0.

[Settings](#)
[Mappings](#)
[Outbound Metadata](#)
[Debug Log](#)

Custom Attributes

Map users into groups according to specified attribute name value pairs.

Edit

4 items

SOURCE	DESTINATION
nameidentifier	sub*
upn	upn*
EmailAddress	email*
Name	displayname

The following attributes are required to properly set up federation on the Delinea Platform:


- **sub: nameidentifier.** The user's unique identifier.
- **upn: upn.** User Principal Name. The user account login name.
- **email: EmailAddress.** The user's email address.

Optionally, these additional user attributes can be mapped on the platform:

- **displayname:** Name (for example, Aditi Patel). While the *displayname* attribute is optional, it is advisable to include it for optimal results.
- **MobileNumber:** The user's mobile phone number.

- **OfficeNumber:** The user's office phone number.
- **HomeNumber:** The user's home phone number.
- **PlatformUserMembershipType:** Indicates whether the user is an Employee or Vendor
- **Description:** Additional descriptive text.

Custom attributes for IdP federation can vary depending on the specific IdP. Consult the documentation and support resources of your chosen IdP.

 **Important:** We recommend against setting up a user account in which the User Principal Names (UPN) serves as the User ID (UUID). UPNs sometimes change, and when a UPN that was serving as a user's UUID changes, the platform creates a new account with no permissions and assigns the existing user to the new account. Therefore that user loses all platform permissions they previously had.

Mapping Federated Groups

Introduction to Group Mapping

Group mapping is a structured approach used to connect user groups from an Identity Provider (IdP), such as Auth0 or Entra ID to corresponding groups on the Delinea Platform (SP). This integration ensures that users receive appropriate access and permissions on the platform based on their group memberships as defined in the IdP. This capability is particularly important in federated authentication scenarios where identity and access management are centralized in the IdP.

How Group Mapping Works

- Administrators define group mappings that link the IdP's user groups to platform groups. These mappings dictate how group attributes received from the IdP are translated to corresponding groups on the Delinea Platform.
- Federated groups are not directly added to named platform identity groups. Instead, each IdP group is identified by a unique Object ID, which the platform uses to establish the mapping.

Authentication Flow for Federated Users

- When a federated user logs in to Delinea Platform, the IdP sends the platform an attribute or claim named groups. This claim includes the Object IDs of the IdP groups to which the user belongs.
- The platform matches these Object IDs to mapped platform groups, automatically assigning the user as a member of the corresponding groups.
- The attribute name depends on the IdP and may be defined by the administrator. Consult your IdP to determine the available options.

Access and Permissions Assignment

- On the Delinea Platform, user access is governed by roles and permissions, which are assigned based on group membership.
- Federated users inherit roles and permissions from the platform groups they are mapped to, ensuring seamless

integration between the federated IdP and the platform's access control model.

- For more details about roles and permissions, refer to the User Roles and Permissions section.

Configuring Group Mapping

Group mapping on the Delinea Platform can be configured in two ways: **manually** or **automatically**. These options provide flexibility for administrators to align the platform's group structure with the Identity Provider's (IdP) attributes and manage user access efficiently.

Manual Group Mapping

Manual mapping allows administrators to define explicit mappings between specific group attributes received from the IdP and local groups on the Delinea Platform.

How It Works:

- Administrators can assign IdP group attributes values (e.g., IT Admin) to corresponding platform groups (e.g., System Administrator).
- The mapping relies on the group attribute name provided by the IdP, which must be specified correctly during configuration.

Example:


A **Group** attribute name with value **IT Admin** received from the IdP is manually mapped to the **System Administrator** local group on the Delinea Platform. This ensures that users belonging to the **IT Admins** group in the IdP are granted the appropriate permissions associated with the **System Administrator** group.

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME ↑	GROUP
<input type="text" value="Group"/>	<input type="text" value="IT Admin"/>	<input type="text" value="System Admin..."/> 

[Add Group Mapping](#)

 **Note:** Group attribute names and values are case-sensitive. When setting up group mappings between the Identity Provider (IdP) and the Delinea Platform, both the **group attribute name** and its **values** are case sensitive and must match exactly.

Automated Group Mapping

Automated group mapping simplifies the process by dynamically creating and assigning groups based on the claims received from the IdP.

How It Works:

- When the **Map Groups Automatically** option is enabled, the Delinea Platform processes group claims sent by the IdP during authentication.

- If a group claim matches a group that does not yet exist on the platform, the platform will automatically create the local group and assign the user to it.
- If no group claim is received, the platform can assign the user to a predefined **fallback group**, ensuring they are granted a baseline level of access.
- If a user's group memberships are updated in the IdP, those changes will automatically be reflected on the Delinea Platform during the user's next login.
- Administrators can later update or modify the user's group memberships as needed.

Key Benefits:

- Reduces manual effort for administrators, especially in dynamic or large-scale environments.
- Ensures new groups and users are incorporated into the platform's access structure without delays.

Example:

When a federated user logs into the Delinea Platform, the platform checks for group attribute name sent by the Identity Provider (IdP). If a matching group is found (e.g., as shown in the example below for Group), the platform automatically creates a platform local group (if it doesn't already exist) based on the group claim value and adds the user to it, simplifying the onboarding process. If no group claims are received, administrators can optionally configure a fallback group to ensure such users are still assigned a baseline level of access.

Group Mappings

Map user to local platform groups according to identity provider (IdP) attributes. [Learn more about Group Mappings](#)

Mapping strategy
Manually align IdP groups to Delinea platform groups or let the platform map it for you.

☐ Map groups manually
☒ Map groups automatically

Group attribute *
Add attribute name

Group

Fallback group
Users will be added to the fallback group if no group claim is received. Otherwise will be added automatically.

Fallback-grp

Choosing Between Manual and Automated Mapping

The choice between manual and automated group mapping depends on your organization's needs:

Manual Mapping:

- Suitable for controlled environments with predefined group structures.
- Provides precise control over group assignments and permissions.

Automated Mapping:

- Ideal for dynamic or federated environments where user groups frequently change or expand.
- Minimizes administrative overhead while maintaining flexibility.

Mapping Federated Users

User mapping enables federated users (from Entra ID, Okta, Ping, etc.) to be recognized by their Active Directory identity after logging in to the Delinea platform. Users authenticating with their AD credential will be recognized by their AD identity instead of as a remote federated user. By mapping to the AD user, privileges are assigned based on AD group memberships, which is easier than mapping federated groups from the SAML provider to the Delinea Platform.

See also [Troubleshooting Federated Group Mapping](#).

Map a federated user to an existing directory user

Required

User Mappings

By default, when a federated user attempts to login, login will fail if a user with the same username exists in another directory service. When this feature is enabled, rather than failing login, the user of the federation will authenticate as the matching user of another directory service.

Map federated user to existing directory user

Required

☒ Create local user if unable to map

☒ Update local users with federated user attributes

Edit

When you select **Required**, you have three additional options:

- **Create local user if unable to map.** If you select this option and an existing user is not found on the platform, a corresponding Delinea Directory user is created, and login is authorized. When the new Delinea local user is generated, it will subsequently be updated with the federated attributes. This functionality facilitates the inbound provisioning of Delinea users from another federation. By default, the attributes of the mapped user take precedence, and the assertions of the federated user are disregarded in future log-ins.
- **Update local users with federated user attributes.** If you select this option, the claims and attributes (for example, MobileNumber) associated with the mapped Delinea Directory (local) user receive regular, consistent updates based on the claims and attributes associated with the federated user.
- **Select neither option.** If you select neither option and no existing platform user matches the federated user, the federated user's platform login attempt will fail, accompanied by an error message similar to the following:

```
{
  "type": "FederationException",
  "title": "I18N_Federation_Exception_CannotMapFederatedUserToDirectoryUser",
  "status": 34,
  "detail": "Federation Default: user 'test@example.com' cannot be mapped to a directory service user.",
  "instance": "/signin-oidc"
}
```

Optional


User Mappings

By default, when a federated user attempts to login, login will fail if a user with the same username exists in another directory service. When this feature is enabled, rather than failing login, the user of the federation will authenticate as the matching user of another directory service.

Edit

Map federated user to existing directory user Optional

If you select **Optional**, when a federation user attempts to authenticate, the platform maps the user to an existing Active Directory account, based on their User Principal Name (UPN). If mapping is not possible, the platform automatically creates a new Federated user to enable a seamless authentication process.

 **Note:** Although the two user objects are mapped, they are not reconciled, so they appear as separate users on the platform.

Disabled

If you select **Disabled** and another user with the same username exists in another directory service, a federated user's login attempt will fail. Below is an example of an error message generated when an attempt to log in to the platform causes a collision between a federated user and one or more other users on the platform with the same UPN.

```
{"type":"FederationException","title":"_I18N_Federation_Exception_UserPrincipalName_Collision","status":31,"detail":"A user named user@example.com already exists in the directory","instance":"/signin-oidc"}
```

Debugging

The Delinea Platform offers a self-service debugging tool for troubleshooting federation setups with IdPs. Administrators can use the debugging tool to independently identify, diagnose, and resolve common problems encountered during the configuration and management of federated authentication systems.

1. On the provider's page, click the **Federation console** tab. You can also access the federation console from various shortcuts.
2. Click the **Start Debugging** button. The indicator next to the button changes from Stopped to Running.
3. Launch a new browser window, preferably in Incognito mode.
4. Navigate to your platform tenant URL.
5. Log in to the platform using a federated account.
6. Upon successful login using the federated account, you can go back to the original platform tab to review the logs captured. Each login event appears in a row displaying session details described in the following table. You can expand the entry to view additional details.

Column	Description
Timestamp	The date and time for the federated user's login event.
Email	Email address associated with the federated user.
UPN	User Principal Name; represents the federated user's identity.
Incoming Attributes	A collection of attributes and values received by the platform from the IdP for the federated user.
Mapped Custom Attributes	Represents the custom destination attributes on the platform and their corresponding values received from the IdP.
Mapped Groups	Contains information about the federated user's group memberships alongside the mapping assignment to local groups on the platform.
Missing Required Attributes	Any mandatory attributes that are missing for the federated user.

Logs are captured up to a limit of 30 minutes. After that, you need to rerun debugging for continued logging. Logs from previous captures are removed at the end of each logging period.

Analyzing Captured Logs

The log provides insight into the following:

- All the claims received from the IdP. Each attribute consists of a key-value pair, where the key represents the attribute name, and the value represents its corresponding value.
- The mapped custom attributes and corresponding values.
- Group mappings, if any. This depends on whether there is a pre-existing configuration for group mappings.
- Flagging of any essential attributes that might be missing.
- A complete log of the SAML request and response.
- Various other information such as Issuer and Entity ID that can aid in troubleshooting.

The following example demonstrates a login request by an Auth0 user to the Delinea Platform.

SAML and OIDC Federation

Incoming Attributes These are the attributes received from the external Identity Provider (IDP). They follow a specific format. Each attribute consists of a key-value pair, where the key represents the attribute name and the value represents its corresponding value.
<ul style="list-style-type: none">• EmailAddress : test@example.com• Group : primary• Name : Test Account From Auth0• authorization : [object Object]• clientId : 2RPKWK6qQPg7tgKQstop0gseym2O3XZh• connection : Username-Password-Authentication• created_at : 2023-03-15T22:29:37.666Z• email_verified : true• isSocial : false• nameidentifier : auth0123456123456ca• nickname : test• provider : auth0• updated_at : 2023-07-19T03:05:29.075Z• upn : test@example.com
Mapped Custom Attributes After undergoing attribute mapping transformation, the attributes are mapped to a standardized format. Each mapped attribute follows a key-value pair structure, where the key represents the custom destination attribute name and the value represents its corresponding value.
<ul style="list-style-type: none">• displayname : Test Account From Auth0• email : test@example.com• sub : auth0_123456123456ca• upn : test@example.com
Mapped Groups After undergoing group mapping transformation, the group values are mapped to a standardized format: The group from the IDP (source) : corresponding mapped Delinea group (destination)
<ul style="list-style-type: none">• primary : System Administrator
Missing Required Attributes Certain attributes are required for successful authentication with the Identity Provider (IDP). If any of these attributes are missing during the authentication process, it may result in an error, and the user will not be able to authenticate with the IDP

Integrating AD FS

This documentation is a detailed guide for setting up single sign-on (SSO) through Active Directory Federation Services (AD FS) leveraging SAML 2.0.



Note: You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

The following procedures require copying and pasting information between AD FS and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

Prerequisites

On the Delinea Platform, you need to be an Admin with federation privileges.

Setting Up AD FS with SAML

Retrieve AD FS metadata

1. Connect to your AD FS server using the following URL:
`https://{FQDN}/FederationMetadata/2007-06/FederationMetadata.xml`

Note: If your metadata file is not available at the URL above, open your AD FS management console, and under **AD FS > Service > Endpoints**, ensure that the Federation Metadata endpoint is enabled.

2. Save the *FederationMetadata.xml* file to a known location.



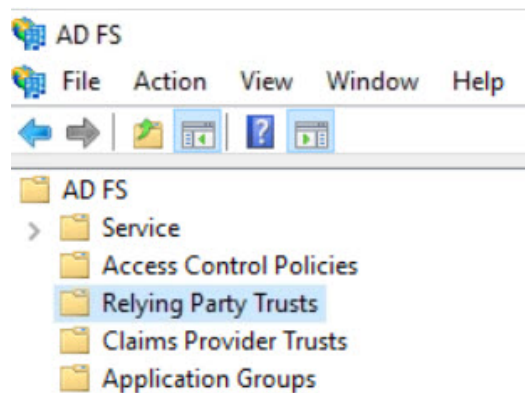
Note: If your metadata file is not available at this URL, open your AD FS management console, and under **AD FS > Service > Endpoints**, ensure that the Federation Metadata endpoint is enabled.

Add the Provider to the platform

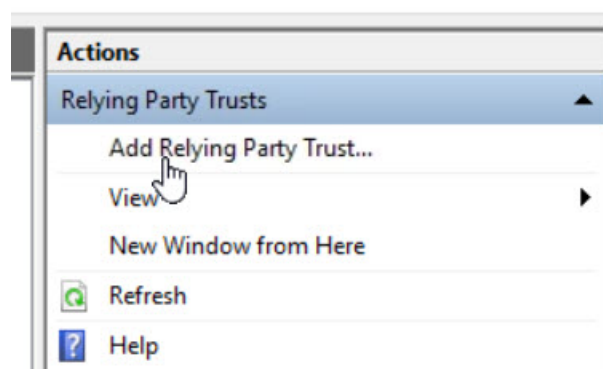
1. Log on to the platform.
2. Click **Settings** from the left navigation menu and select **Federation providers**.
3. On the Federation Providers page, click **Add Provider** and select **SAML** from the drop-down menu.
4. On the **Add Provider** page next to **SAML provider configuration**, click **Select file**.
5. Find and select the AD FS metadata file you downloaded, then click **Upload SAML configuration**.
6. On the **SAML Provider Settings** page, click **Edit** to update the data that was auto-generated from metadata.
7. Update the **Name** field with a meaningful name.
8. Optionally, select the **Enabled** box next to **Status**.
9. In the **Advanced Settings** section:
 - a. Select the box next to **Customize Issuer Sent To IDP** (you can leave the field as is, but the option must be enabled).
 - b. Select the box next to **Sign Request**.
 - c. Next to **Request signing certificate**, click **Select file**.
 - d. Browse to and select a valid pfx file.
 - e. Enter your pfx password in the **Password** field.
10. In the **Domains** section, add one or more domains that should be managed by this SAML provider.
11. Click **Save**.

Initial AD FS Setup

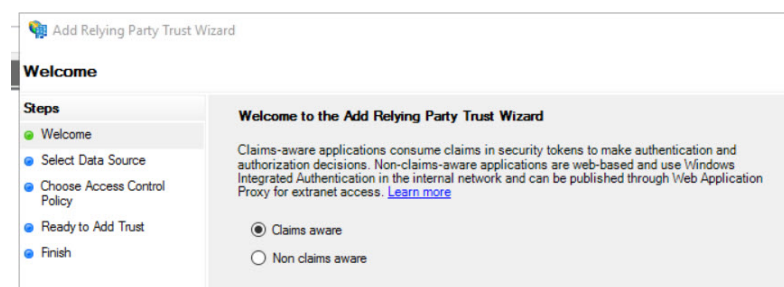
1. Open the AD FS Management console.
2. From the left tree view, select **Relying Party Trusts**.



3. From the right panel, click **Add Relying Party Trust...**



4. Select **Claims aware**.



5. Click **Start**.
6. Select **Import data about the relying party from a file**.
7. Click **Browse** to select the xml file you downloaded from the platform.

8. Click **Next**.

Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

C:\Users\Administrator\Downloads\FederationMetadata.xml **Browse...**

☐ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

9. Enter a meaningful **Display name**.

Add Relying Party Trust Wizard

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Enter the display name and any optional notes for this relying party.

Display name:

Delinea Platform

Notes:

10. Click **Next**.

11. Choose an access control policy such as **Permit Everyone**, and click **Next**.

Add Relying Party Trust Wizard

Choose Access Control Policy

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more...

Policy

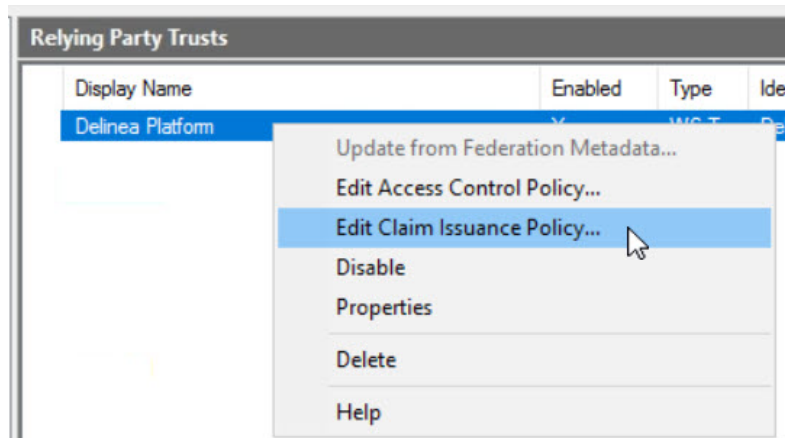
Permit everyone

12. On the **Ready to Add Trust** screen, click **Next**.

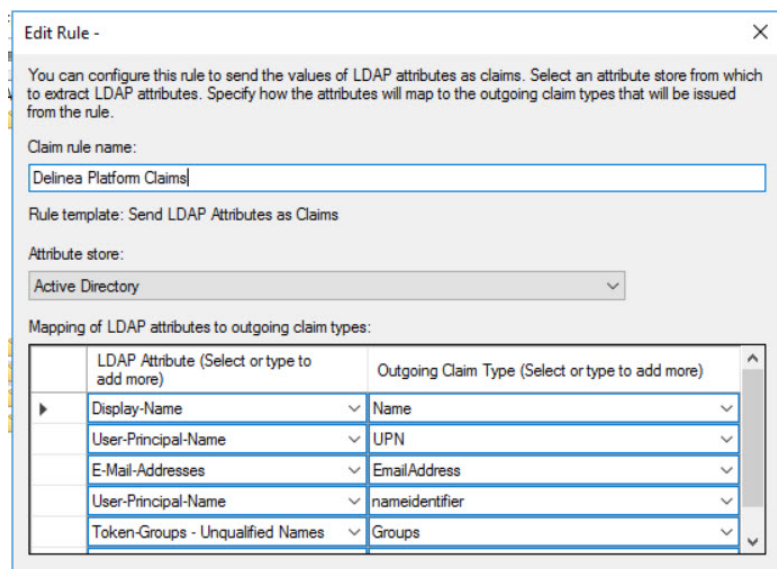
13. Ensure that the box is selected next to **Configure claims issuance policy for this application**.
14. Click **Finish**.

Configure assertion attributes

1. Right click the newly created **Relying Party Trust**, and click **Edit Claim Issuance Policy**.



2. From the Claim Issuance Policy editor, click **Add Rule**.
3. Select **Send LDAP attributes as Claims**.
4. Click **Next**.
5. Enter a meaningful rule name (e.g. *Delinea Platform Claims*).
6. For **Attribute Store**, select **Active Directory**(or any LDAP server you may use).
7. Map attributes from your directory to the claim names expected by the platform.



By default, the platform expects the following claims:

- **sub: nameidentifier.** The user's unique identifier.
- **upn: upn.** User Principal Name. The user account logon name.
- **email: EmailAddress.** The user's email address.
- **displayname: Name.** The user's name for display purposes (optional, but recommended).

Attribute Mappings

You can add or modify expected claims from the platform federation settings, under **Attribute Mappings**.

If you want to leverage the group mapping feature and give different permissions to the authenticated user based on the user's groups, you can also add a groups claim or similar and map it to the Token Groups - Unqualified Names AD attribute. From the platform, go into your Federation settings and configure **Group Mappings**.

8. Below is an example that grants Delinea Platform admin rights to any user belonging to the PAM-ADMIN group:

The screenshot shows the 'Azure AD FS' Federation console. It has tabs for 'Settings' and 'Federation console'. A 'Delete' button is in the top right. The 'Attribute Mappings' section explains that user attributes are passed from the identity provider (IdP) to the Delinea Platform (SP). It contains a table with columns 'SOURCE' and 'DESTINATION'. The table lists four mappings: EmailAddress to email, Name to displayname, nameidentifier to sub, and upn to upn. Each mapping has a 'Required Attribute' button. Below this is the 'Group Mappings' section, which explains that users are mapped into groups based on attribute values. It contains a table with columns 'ATTRIBUTE', 'SOURCE NAME', and 'GROUP'. The table shows a mapping for 'Groups' with source name 'PAM-ADMIN' and group 'System Administrator'.

SOURCE	DESTINATION
EmailAddress	email
Name	displayname
nameidentifier	sub
upn	upn

ATTRIBUTE	SOURCE NAME	GROUP
Groups	PAM-ADMIN	System Administrator

9. Click **OK**, then click **OK** again.

Add the Provider to the Platform

1. Log on to the platform.
2. Click **Settings** from the left navigation menu and select **Federation providers**.
3. On the Federation Providers page, click **Add Provider** and select **SAML** from the drop-down menu. The **Add Provider** page opens.

Settings

In the Settings section, the first fields are automatically populated when you select the SAML provider configuration file and click **Apply**.

1. Next to **SAML provider configuration**, click **Select file**.
2. Find and select the AD FS metadata file you downloaded.

3. Click **Upload SAML configuration**. The word, *Apply* appears above the right end of the SAML provider configuration field. then
4. Click **Apply**. The words *Uploaded successfully* will appear next to SAML provider configuration, and the empty fields below will be auto-populated:
 - **Name**: Auto-generated from metadata
 - **Protocol**: SAML (auto-filled)
 - **Status**: Disabled
 - **Entity ID** [example: `https://sts.windows.net/808444af-4011-40d5-9b0a-a9a5c95f88e9/`]
 - **IDP Certificate**: Click **Select File**, then navigate to and select the Signing Certificate file you downloaded, to populate the following fields:
 - Signature
 - Algorithm
 - Thumbprint
 - Not valid before
 - Not valid after
 - Issuer
5. **IDP Login URL**: Paste in the Login URL from your new IdP SAML application.
6. **IDP Logout URL**: Paste in the Logout URL from new IdP SAML application.
7. **Platform Callback URL**: `https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer` Copy the Platform Callback URL to paste into the appropriate field in your new IdP SAML application.
8. **Platform Logout URL**: `https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer`
9. **Status**: Select the box next to **Enabled**.

Advanced Settings

1. Select the box next to **Customize Issuer Sent To IDP** (you can leave the field as is, but the option must be enabled).
2. Select the box next to **Sign Request**.
3. Next to **Request signing certificate**, click **Select file**.
4. Browse to and select a valid pfx file.
5. Enter your pfx password in the **Password** field.

Also see "Advanced Settings (SAML only)" on page 374 under Federation Management.

Attribute Mappings

See "Attribute Mappings" on page 376 under Federation Management.

Group Mappings

See "Mapping Federated Groups" on page 377 under Federation Management.

User Mappings

See "Mapping Federated Users" on page 380 under Federation Management.

Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.
2. Optionally enable the Status of the provider.
3. When all required fields are populated, click **Add Provider**.

Integrating Auth0

This documentation is a detailed guide for setting up single sign-on (SSO) through Auth0, leveraging SAML 2.0 or OIDC.

The following procedures require copying and pasting information between Auth0 and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.



Note: You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

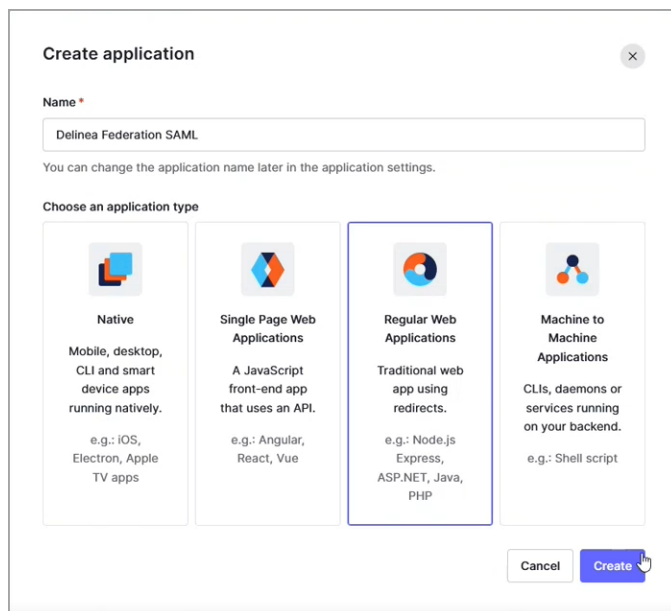
Prerequisites

On the Delinea Platform, you need to be an Admin with federation privileges.

Build an Auth0 SAML Application

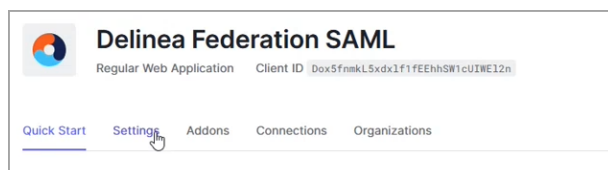
1. From the left navigation menu, click **Applications**.
2. On the Applications page, click **Create Application**.

SAML and OIDC Federation



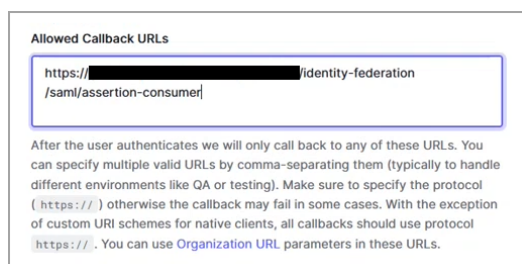
The 'Create application' dialog box has a title bar with a close button. It contains a 'Name' field with the text 'Delinea Federation SAML'. Below this is a note: 'You can change the application name later in the application settings.' Under the heading 'Choose an application type', there are four cards: 'Native' (Mobile, desktop, CLI and smart device apps running natively. e.g.: iOS, Electron, Apple TV apps), 'Single Page Web Applications' (A JavaScript front-end app that uses an API. e.g.: Angular, React, Vue), 'Regular Web Applications' (Traditional web app using redirects. e.g.: Node.js Express, ASP.NET, Java, PHP), and 'Machine to Machine Applications' (CLIs, daemons or services running on your backend. e.g.: Shell script). The 'Regular Web Applications' card is selected with a blue border. At the bottom right are 'Cancel' and 'Create' buttons.

3. On the Create Application page, enter a name for your Auth0 new SAML application, such as Auth0 SAML.
4. Choose **Regular Web Applications**.
5. Click **Create**.
6. On your Auth0 new SAML application page, click the **Settings** tab.



The application settings page for 'Delinea Federation SAML' is shown. It includes the Auth0 logo, the application name, type ('Regular Web Application'), and a 'Client ID'. A navigation bar at the bottom has tabs for 'Quick Start', 'Settings' (which is selected), 'Addons', 'Connections', and 'Organizations'.

7. Scroll down to **Allowed Callback URLs**.
8. Paste the following: ``https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer``
9. Replace [HOST-NAME] with the host name you selected when you created your tenant.

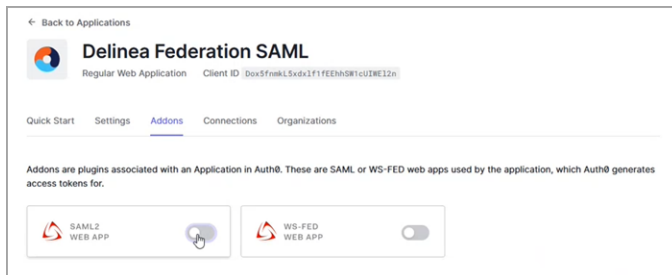


The 'Allowed Callback URLs' section shows a text input field containing the URL `https://[REDACTED].delinea.app/identity-federation/saml/assertion-consumer/`. Below the field is explanatory text: 'After the user authenticates we will only call back to any of these URLs. You can specify multiple valid URLs by comma-separating them (typically to handle different environments like QA or testing). Make sure to specify the protocol (https://) otherwise the callback may fail in some cases. With the exception of custom URI schemes for native clients, all callbacks should use protocol https:// . You can use Organization URL parameters in these URLs.'

10. Click **Save Changes**.
11. Click the **Add ons** tab.

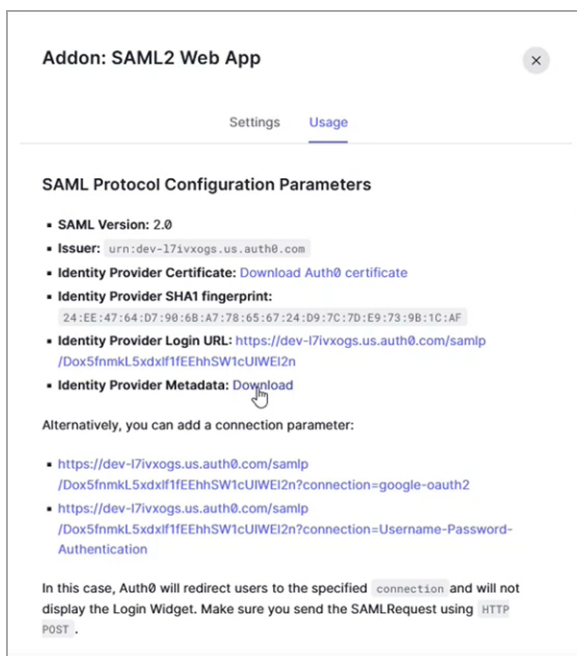
SAML and OIDC Federation


- Click the toggle to enable SAML 2.



The **Addon: SAML2 Web App** page opens.

- From the **Usage** tab, next to **Identity Provider Metadata** and **Identity Provider Certificate**, click **Download**.



 **Note:** Identity Provider Metadata is an XML-formatted document that contains configuration information necessary for Delinea Federation to authenticate against the identity provider and includes the required endpoint URLs, bindings, and certificates.

- Click the **Settings** tab.
- Scroll to the bottom and click **Enable**.
- Click **Save**.

Add the Provider to the Platform

- Log on to the platform,
- Click **Settings** from the left navigation, then click **Federation Providers**.

3. Click **Add Provider**.
4. Select **SAML** from the drop-down menu. The **Add Provider** page opens.

Settings

In the **Settings** section, the first fields are automatically populated when you select the SAML provider configuration file and click **Apply**.

1. **SAML provider configuration:** Click **Select file**.
2. Navigate to and select the federation metadata XML file you downloaded.
The word, **Apply** appears above the right end of the SAML provider configuration field.
3. Click **Apply**. The words *Uploaded successfully* will appear next to SAML provider configuration, and the empty fields below will be auto-populated:
 - **Name:** Auto-generated from metadata
 - **Protocol:** SAML (auto-filled)
 - **Status:** Disabled
 - **Entity ID** [example: `https://sts.windows.net/808444af-4011-40d5-9b0a-a9a5c95f88e9/`]
 - **IDP Certificate:** Click **Select File**, then navigate to and select the Signing Certificate file you downloaded, to populate the following fields:
 - Signature
 - Algorithm
 - Thumbprint
 - Not valid before
 - Not valid after
 - Issuer
4. **IDP Login URL:** Paste in the Login URL from your Auth0 application.
5. **IDP Logout URL:** Paste in the Logout URL from your Auth0 application.
6. **Platform Callback URL:** `https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer`. Copy the Platform Callback URL to paste into the Allowed Callback URLs field in your Auth0 application.
7. **Platform Logout URL:** `https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer`
8. **Status:** Select the box next to Enabled.

Advanced Settings

See "Advanced Settings (SAML only)" on page 374 under Federation Management.

Attribute Mappings

See "Attribute Mappings" on page 376 under Federation Management.

Adding Custom Claims

See the following references for information on adding custom claims for Auth0:

[Create Custom Claims](#)

[Sample Use Cases: Scopes and Claims](#)

Group Mappings

See "Mapping Federated Groups" on page 377 under Federation Management.

User Mappings

See "Mapping Federated Users" on page 380 under Federation Management.

Domains

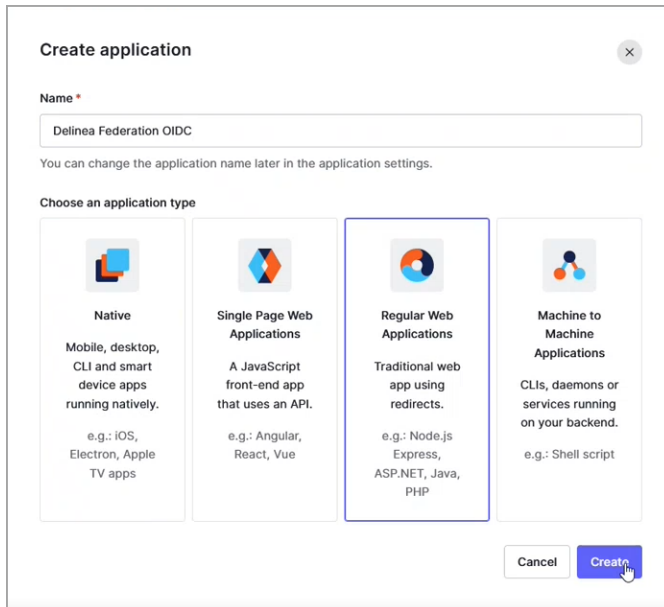
1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.
2. Optionally enable the Status of the provider.
3. When all required fields are populated, click **Add Provider**.

Build an Auth0 OIDC Application



Note: The following procedure requires copying and pasting information between Auth0 and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

1. From the left navigation menu, click **Applications**.
2. On the **Applications** page, click **Create Application**.
3. On the **Create application** page, enter a name for your Auth0 new OIDC application.




Create application

Name *

Delinea Federation OIDC

You can change the application name later in the application settings.


Choose an application type



Native

Mobile, desktop, CLI and smart device apps running natively.


e.g.: iOS, Electron, Apple TV apps



Single Page Web Applications

A JavaScript front-end app that uses an API.


e.g.: Angular, React, Vue



Regular Web Applications

Traditional web app using redirects.

e.g.: Node.js Express, ASP.NET, Java, PHP



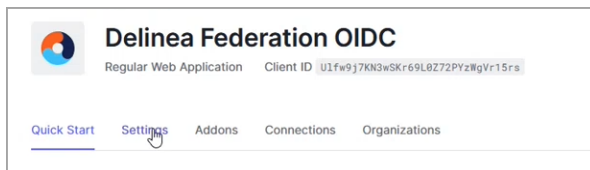
Machine to Machine Applications

CLIs, daemons or services running on your backend.

e.g.: Shell script

Cancel Create

4. Select **Regular Web Applications**.
5. Click **Create**.
6. On your Auth0 new OIDC application page, click the **Settings** tab.




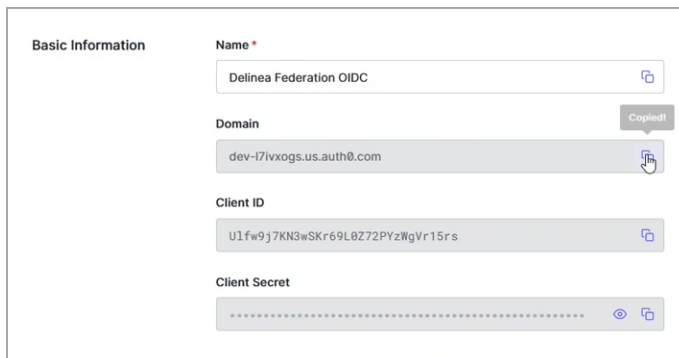
Delinea Federation OIDC

Regular Web Application Client ID U1fw9j7KN3wSKr69L0Z72PYzWgVr15rs

Quick Start **Settings** Addons Connections Organizations

7. Scroll down to the **Basic Information** section.

 **Note:** In the next steps, you will copy the **Domain**, **Client ID**, and **Client Secret** from the Basic Information fields shown below, and paste them into fields on your Delinea Platform.



Basic Information

Name *

Delinea Federation OIDC

Domain

dev-17ivxogs.us.auth0.com

Client ID

U1fw9j7KN3wSKr69L0Z72PYzWgVr15rs

Client Secret

.....

Add the Provider to the Platform

1. Click **Settings** from the left navigation, then click **Federation Providers**.
2. Click **Add Provider**.
3. Select **OIDC** from the drop-down menu. The **Add Provider** page opens.

Settings

1. **Name:** Enter a unique name.
2. **Status:** Select the box next to **Enabled**.
3. **Endpoint URL:** Paste the URL from your Auth0 new OIDC application page **Domain** field.
4. **Client ID:** Paste the Client ID from your Auth0 new OIDC application page.
5. **Client Secret:** Paste the Client Secret from your Auth0 new OIDC application page.
6. **Prompt:** See ["Prompt for Re-authentication \(OIDC only\)" on page 375](#) under Federation Management.
7. **Platform Callback URL:** Copy the Callback URL. On your Auth0 new OIDC application page, scroll to Application URLs and paste the copied callback URL into the Allowed Callback URLs field.

Attribute Mappings

See ["Attribute Mappings" on page 376](#) under Federation Management.

Group Mappings

Also see ["Mapping Federated Groups" on page 377](#) under Federation Management.

User Mappings

See ["Mapping Federated Users" on page 380](#) under Federation Management.

Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.
2. Optionally enable the Status of the provider.
3. When all required fields are populated, click **Add Provider**.

Integrating BlokSec

BlokSec is the leading provider of passwordless Immutable Authentication™ services, designed to combat password-based attacks, account takeovers, phishing, online fraud, and identity theft. These solutions are essential for organizations aiming to implement Zero Trust Network.

The following BlokSec integration is available:

[Integrating Passwordless Authentication with the Delinea Platform](#)

Integrating Celestix

Celestix Networks is a network security provider specializing in remote access, authentication, and cutting-edge solutions like Zero Trust. Celestix Networks aims to simplify security, providing peace of mind and freedom from restrictions in a rapidly evolving digital world.

The following Celestix integration is available:

[Integrating Celestix V-Key with the Delinea Platform](#)

Integrating Entra ID



Note: At the end of 2023, Microsoft completed the change of their product name from *Microsoft Azure Active Directory* (Azure AD or ADD) to *Microsoft Entra ID* (Entra or Entra ID).

This documentation is a detailed guide for setting up single sign-on (SSO) through Entra ID, leveraging SAML 2.0 or OIDC.

The following procedures require copying and pasting information between Entra and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.



Note: You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.



Note: Instead of using Entra ID federation as described in this topic, you can use Entra ID as a Registered App (native integration). See [API-Based Integration with Entra ID](#). But you cannot use both features simultaneously with the same domains.

Prerequisites

On the Delinea Platform, you need to be an Administrator with federation privileges.

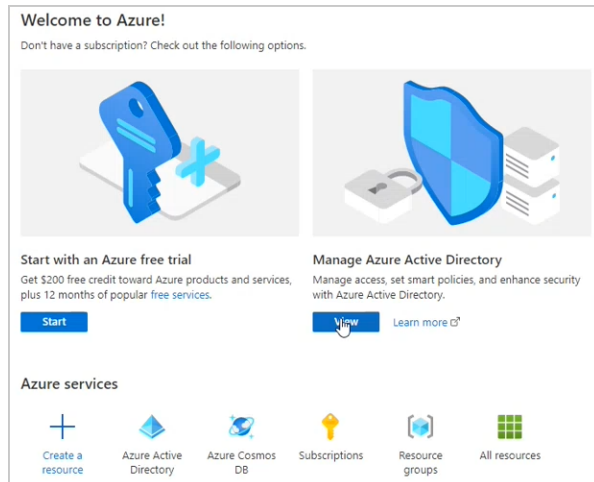
Decide whether you will be using SAML or OIDC.

- For SAML, see "Build an Entra SAML Application" below and "Add the SAML Provider to the Platform " on page 404.
- For OIDC, see "Build an Entra OIDC Application" on page 406 and "Add the OIDC Provider to the Platform " on page 409.

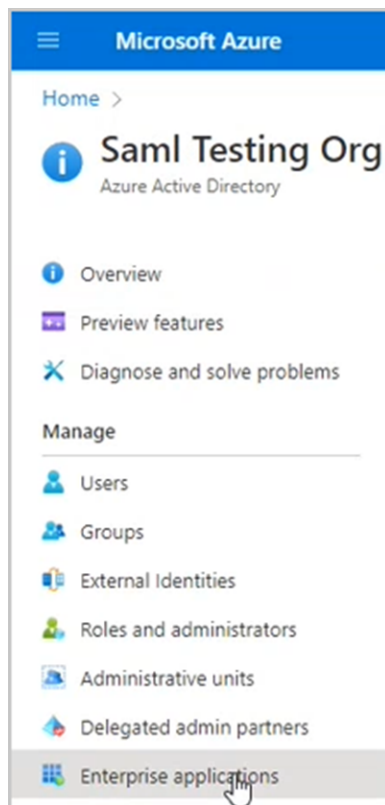
Build an Entra SAML Application

1. Log into the Entra ID portal at <https://portal.azure.com/>.
2. Under **Manage Azure Active Directory**, click **View**.

SAML and OIDC Federation

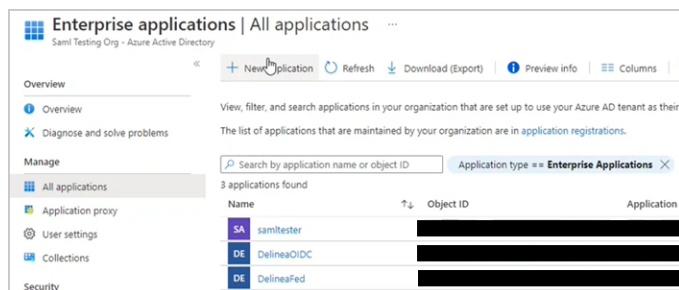


- From the left panel, click **Enterprise Applications**.

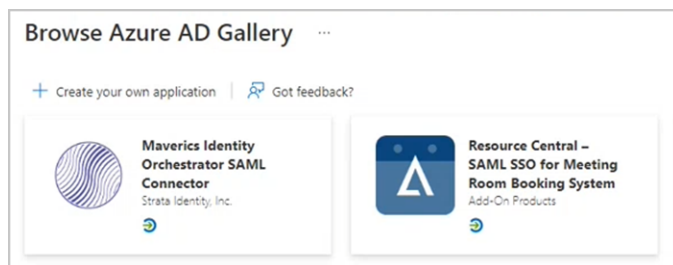


- From the top row, click **+ New Application**.

SAML and OIDC Federation



- At the top of the **Browse Microsoft Entra ID Gallery** page, click **Create your own application**.

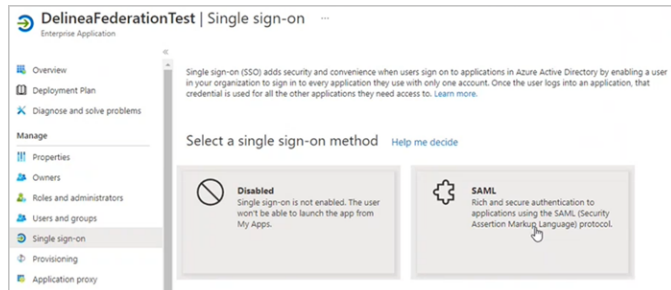


- On the **Create your own application** page:

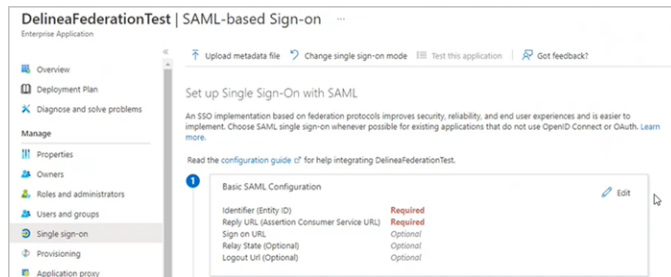
The screenshot shows the 'Create your own application' form. It has a title bar with a close button. Below the title, there is a 'Got feedback?' link. The main text says: 'If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.' There is a text input field for 'What's the name of your app?' with the value 'DelineaFederationTest' and a green checkmark. Below this, there is a section 'What are you looking to do with your application?' with three radio button options: 'Configure Application Proxy for secure remote access to an on-premises application', 'Register an application to integrate with Azure AD (App you're developing)', and 'Integrate any other application you don't find in the gallery (Non-gallery)'. The third option is selected. At the bottom, there is a blue 'Create' button.

- Enter a meaningful name (for example, Delinea Federation).
 - Ensure this option is selected: **Integrate any other application you don't find in the gallery (Non-gallery)**.
 - Click **Create**.
- Once your application is created, click **Single sign-on** from the left panel.
 - Click the SAML card.

SAML and OIDC Federation



9. On the SAML-based Sign-on page, click **Edit** at the top right of the **Basic SAML Configuration** block



10. In the Basic SAML Configuration panel that appears on the right side, click **Add Identifier**.

The screenshot shows the 'Basic SAML Configuration' panel. It has a 'Save' button and a 'Got feedback?' link. Below this is a message: 'Want to leave this preview of the SAML Configuration experience? Click here to leave the preview.' The panel contains several sections: 'Identifier (Entity ID)' with a description and an 'Add identifier' link; 'Reply URL (Assertion Consumer Service URL)' with a description and an 'Add reply URL' link; 'Sign on URL (Optional)' with a description and a text input field; 'Relay State (Optional)' with a description and a text input field; and 'Logout URL (Optional)' with a description and a text input field. Each text input field has a green checkmark icon on the right.

11. Add the following values:

SAML and OIDC Federation

Basic SAML Configuration

Save | Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) * ⓘ

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant. The default identifier will be the audience of the SAML response for IDP-initiated SSO.

Default

CN=Microsoft:Azure:Federated:SSO:Certificate

Add identifier

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer

Add reply URL

Sign on URL (Optional)

Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Enter a sign on URL

- Identifier (Entity ID)** This value must be unique, for example 'CN=Microsoft:Azure:Federated:SSO:Certificate' or you may enable **Customize certificate issuer sent to IDP** in [Advanced Settings](#) and use that value.
- Reply URL (Assertion Consumer Service URL)**
https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer
Replace [HOST-NAME] with the host name you selected when you created your tenant.
- Logout URL (Optional)**
https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer
Replace [HOST-NAME] with the host name you selected when you created your tenant.
- Click **Save** at the top left.

Attributes and Claims Mappings

- Click **Edit** at the right side of the **Attributes & Claims** block.

Attributes & Claims

givenname	user.givenname
surname	user.surname

Edit

There are four (4) claims the Delinea Platform requires:

Source | Destination (see steps 6 and 8 for details)

- EmailAddress | email
- Name | displayname
- nameidentifier | user.objectid
- upn | upn

SAML and OIDC Federation

2. In the **Attributes & Claims** dialog, click the Name claim as shown below and change the Source attribute to `user.displayName`.

`http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`
Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [...]

Additional claims

Claim name	Type	Value
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress</code>	SAML	user.mail ***
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname</code>	SAML	user.givenname ***
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</code>	SAML	user.userprincipalname ***
<code>http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname</code>	SAML	user.surname ***

^ Advanced settings

Advanced SAML claims options [Edit](#)

3. Click **Save**.
4. As needed, add the groups assigned to this application as a claim in the SAML token.
5. Click **Add new claim**.
6. On the **Manage Claim** page, enter the following values:
 - **Name:** `nameidentifier`
 - **Source Attribute:** `user.objectid`

Manage claim ...

[Save](#) [Discard changes](#) | [Got feedback?](#)

Name * ✓

Namespace ✓

Choose name format

Source * ☒ Attribute ☐ Transformation
☐ Directory schema extension (Preview)




Source attribute * ✓

Claim conditions

7. Click **Save**.
8. Add a second claim for the for upn using the following values:
 - **Name:** `upn`
 - **Source Attribute:** `user.userprincipalname`

SAML and OIDC Federation

Manage claim ...

 Save  Discard changes  Got feedback?

Name * ✓

Namespace ✓

Choose name format (Preview)

Source * ☒ Attribute ☐ Transformation

Source attribute * ✓

Claim conditions

9. Click **Save**. Your final claims appear.

Attributes & Claims ...

[+ Add new claim](#) [+ Add a group claim](#) [Columns](#) [Got feedback?](#)

Required claim

Claim name	Type	Value
Unique User Identifier (Name ID)	SAML	user.userprincipalname [na... ***

Additional claims



Claim name	Type	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	SAML	user.mail ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	SAML	user.givenname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	SAML	user.displayname ***
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	SAML	user.surname ***
nameidentifier	SAML	user.objectid ***
upn	SAML	user.userprincipalname ***

10. Click the **SAML-based Sign-on** link to go back to the SAML setup screen.



11. In the **SAML Certificates** block, click **Download** next to **Federation Metadata XML** and **Certificate (Base64)**

3 SAML Certificates

Token signing certificate		
Status	Active	
Thumbprint	D21CE1748394AA5E6A3284F8B79A559EB45EF53	
Expiration	11/21/2025, 10:07:13 AM	
Notification Email	[REDACTED]	
App Federation Metadata Url	https://login.microsoftonline.com/0131dddc-4b37...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	
Verification certificates (optional) (Preview)		
Required	No	
Active	0	
Expired	0	

You will use these saved files in the next step to configure the Federation service in your Delinea tenant.

Add the SAML Provider to the Platform

1. Log in to the Delinea Platform.
2. Click **Settings** from the left navigation, then click **Federation Providers**.
3. Click **Add Provider**.
4. Select **SAML** from the drop-down menu. The **Add Provider** page opens.

Settings

In the Settings section, the first fields are automatically populated when you select the SAML provider configuration file and click **Apply**.

1. **SAML provider configuration:** Click **Select file**.
2. Navigate to and select the federation metadata XML file you downloaded. *Apply* appears above the right end of the SAML provider configuration field.
3. Click **Apply**. The words *Uploaded successfully* will appear next to SAML provider configuration, and the empty fields below will be auto-populated:
 - **Name:** Auto-generated from metadata
 - **Protocol:** SAML (auto-filled)
 - **Status:** Disabled
 - **Entity ID** [example: `https://sts.windows.net/808444af-4011-40d5-9b0a-a9a5c95f88e9/`]
 - **IDP Certificate:** Click **Select File**, then navigate to and select the Signing Certificate file you downloaded, to populate the following fields:
 - Signature
 - Algorithm
 - Thumbprint
 - Not valid before
 - Not valid after
 - Issuer
4. **IDP Login URL:** Paste in the **Login URL** copied from your application in Entra, Step 4.

4 Set up DelineaFederationTest

You'll need to configure the application to link with Microsoft Entra ID.

Login URL	<code>https://login.microsoftonline.com/808444af-4011-...</code>
Microsoft Entra Identifier	<code>https://sts.windows.net/808444af-4011-40d5-9b0...</code>
Logout URL	<code>https://login.microsoftonline.com/808444af-4011-...</code>

5. **IDP Logout URL:** Paste in the **Logout URL** copied from your application in Entra, Step 4.

6. **Platform Callback URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/assertion-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer)
Copy the Platform Callback URL and paste into the appropriate field in your new Entra application.
7. **Platform Logout URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/logout-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer)
8. **Status:** Select the box next to Enabled.

Advanced Settings

See "Advanced Settings (SAML only)" on page 374 under Federation Management.

Attribute Mappings


- EmailAddress | email
- Name | displayname
- nameidentifier | sub
- upn | upn

Group Mappings


1. Click **Add Group Mapping**.
2. Under **Attribute**, enter the character string '*groups*' exactly as it appears between the single quotation marks, all lowercase.
3. Under **Source Name**, enter the **Object ID** copied from the appropriate group on the Microsoft Entra ID Groups page.

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME ↑	GROUP
<input type="text" value="groups"/>	<input type="text" value="4896efcb-ace-4bb0-b25d-f52"/>	<input type="text" value="Search or pick ..."/> 

[Add Group Mapping](#)



GLOBAL ADMINS

Security Group for Global Administration

Membership type	<input type="text" value="Assigned"/>
Source	<input type="text" value="Cloud"/>
Type	<input type="text" value="Security"/> Copied
Object id	<input type="text" value="4896efcb-ace9-4bb0-b25d-f52a6"/>
Created at	<input type="text" value="6/30/2023, 1:28:43 PM"/>

SAML and OIDC Federation

4. From the **Groups** drop-down, select a group from the pull-down menu. (You can use the *groups* attribute to map more than one group.)

Also see "Mapping Federated Groups" on page 377 under Federation Management.

User Mappings

See "Mapping Federated Users" on page 380.

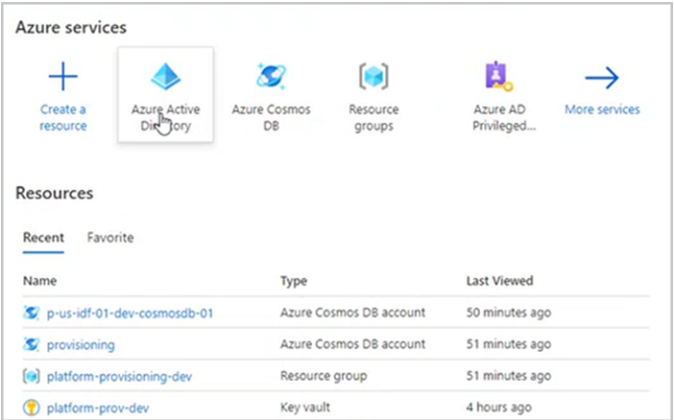
Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.
2. When all required fields are populated, click **Save**.

Build an Entra OIDC Application

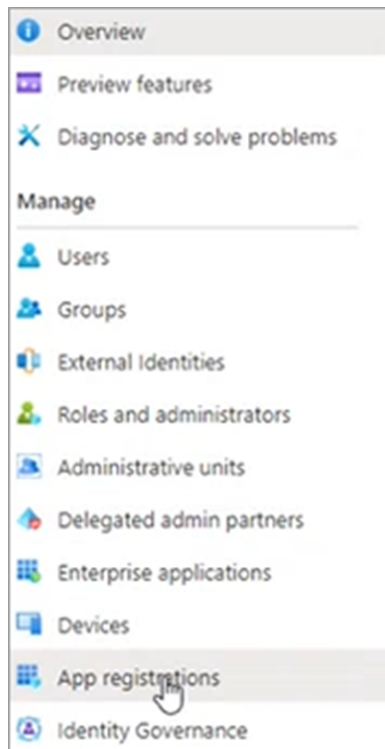
If you chose not to use SAML (described in the previous section, "Build an Entra SAML Application" on page 397), use the following technique to build an OIDC application.

1. Log into the Entra ID portal.
2. From the Entra ID Home page, click the **Entra ID** icon.

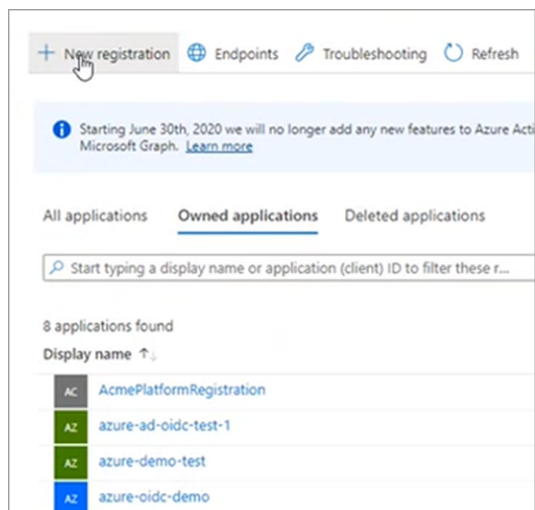


3. Once inside the Entra ID service, click **App Registrations** from the left navigation.

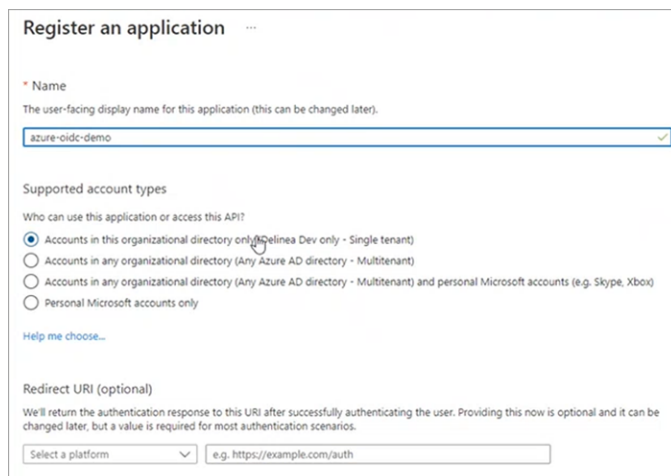
SAML and OIDC Federation



4. Along the top row, click **+ New Registration**.



The **Register an application** page appears.



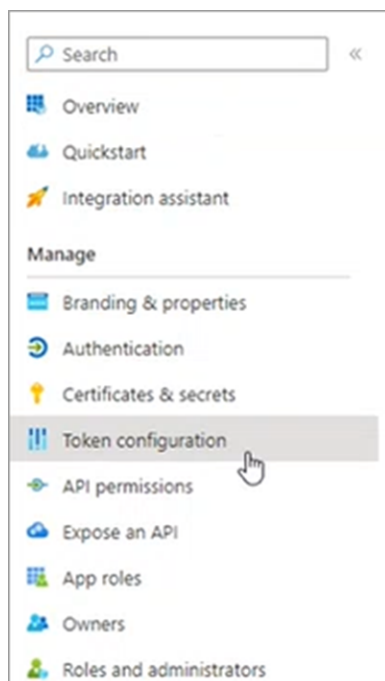
The screenshot shows the 'Register an application' form. It includes a 'Name' field with the value 'azure-oidc-demo'. Below this is a section for 'Supported account types' with four radio button options. The first option, 'Accounts in this organizational directory only (Delinea Dev only - Single tenant)', is selected. A 'Help me choose...' link is provided. At the bottom, there is a 'Redirect URI (optional)' section with a dropdown menu set to 'Select a platform' and a text input field containing 'e.g. https://example.com/auth'.

5. Fill out the fields as follows:

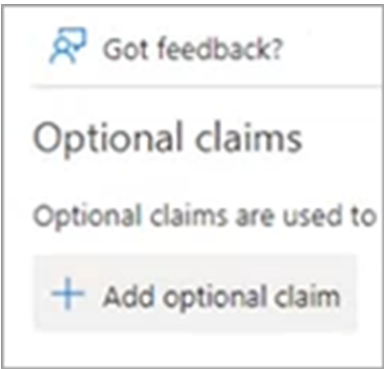
- **Name:** Give the new application you are registering a name. Any descriptive name works. This name will be displayed to users by Microsoft during the first login but it does not matter to the Delinea Platform. For demonstration purposes, we will use the name `azure-oidc-testdemo`
- **Supported account types:** Click the one with *Single tenant* in its name. To see the difference between the account types, click **Help me choose...**
- **Redirect URL:** This can be added in a later step.

6. Click **Register** at the bottom left.

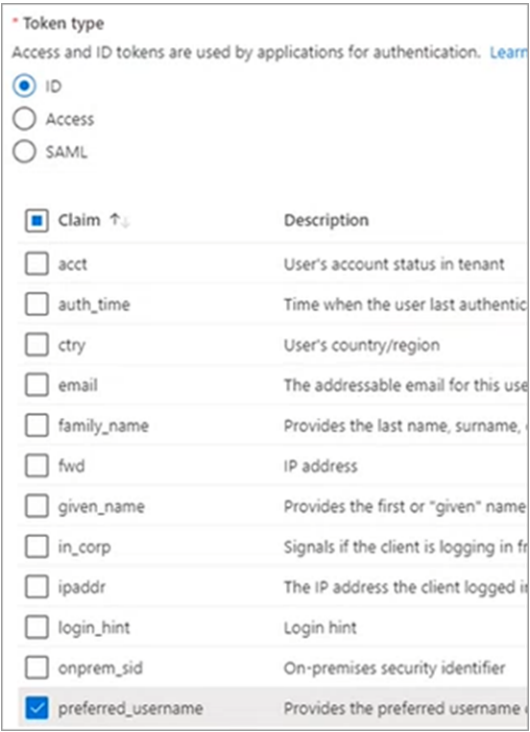
7. From the left navigation, click **Token Configuration**.



8. Click **Add optional claim**.



A panel opens on the right side.



- Under **Token Type**, click **ID**.
- Under **Claim**, click **preferred_username**.

9. Click **Add** at the bottom left.

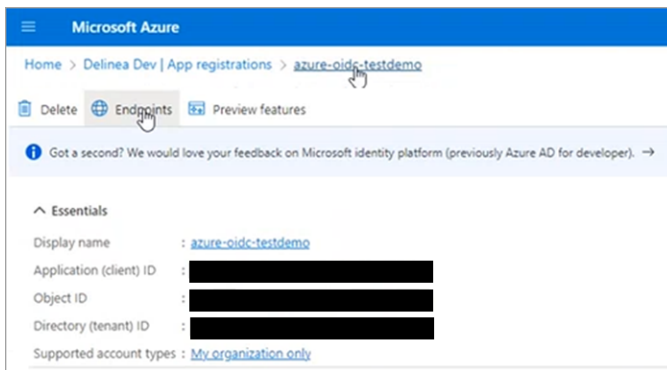
Add the OIDC Provider to the Platform

1. Log on to the platform.
2. Click **Settings** from the left navigation, then click **Federation Providers**.

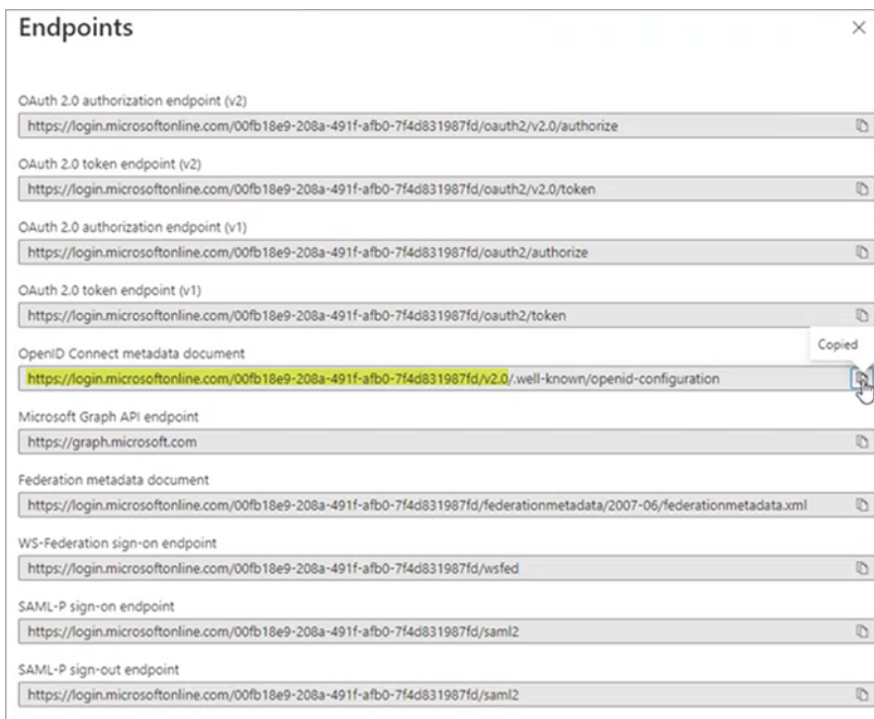
3. Click **Add Provider**.
4. Select **OIDC** from the drop-down menu. The **Add Provider** page opens.

Settings

1. **Name:** Enter a unique name.
2. **Status:** Select the box next to **Enabled**.
3. **Endpoint URL:** This URL is based on your Entra ID tenant ID. To retrieve your Entra ID tenant ID:
 - a. Return to your Entra ID app page and click **Endpoints** at the top of the page.



- b. From the panel that opens to the right, select the URL below **OpenID Connect metadata document**
- c. Copy the entire URL **only up to v2.0**. The value will be `https://login.microsoftonline.com/[TenantId]/v2.0`. See the image below.



4. Paste the copied portion of the URL into the **Endpoint URL** field on the platform.
5. **Client ID:** Copy this value from your new Entra application page next to **Application (client) ID** and paste it into the **Client ID** field on the platform **+Add Federation Service** page.
6. **Client Secret:**
 - a. Return to your new Entra application page.
 - b. Click **Certificates & Secrets** from the left navigation.
 - c. Click **+ New client secret**.
 - d. In the panel that opens to the right, fill in the fields for **Description** and **Expires**.
 - e. Click **Add** at the bottom. A secret value is generated.
 - f. Copy the Secret value from the **Value** field.
 - g. Paste the value into the **Client Secret** field on the platform **Add Provider** page.
7. **Prompt:** See "Prompt for Re-authentication (OIDC only)" on page 375 under Federation Management.
8. **Platform Callback URL:** Copy the platform callback URL and paste it into the Redirect URIs field in your new Microsoft Entra ID application.

Attribute Mappings

Some defaults are provided but can be overridden as needed. In this example we will replace the upn value with preferred_username.

SAML and OIDC Federation

- <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress> | email
- name | displayname
- <http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier> | sub
- preferred_username | upn

Group Mappings

1. Click **Add Group Mapping**.

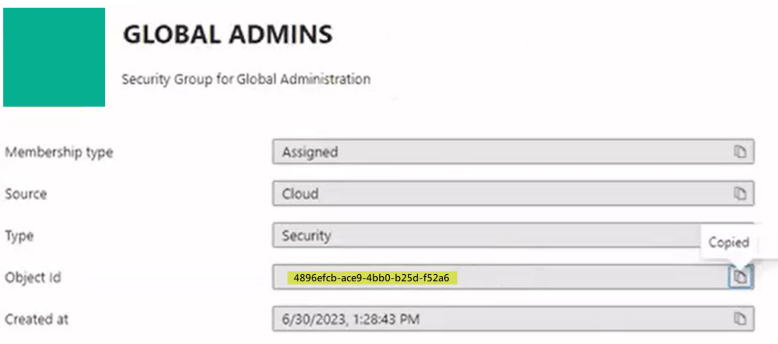
2. Under **Attribute**, enter the character string '*groups*' exactly as it appears between the single quotation marks, all lowercase.
3. Under **Source Name**, enter the **Object ID** copied from the appropriate *groups* on the Microsoft Entra ID Groups page.

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME ↑	GROUP
<input type="text" value="groups"/>	<input type="text" value="4896efcb-ace-4bb0-b25d-f52"/>	<input type="text" value="Search or pick ..."/>

[Add Group Mapping](#)



4. Under the **Group** drop-down, select a group from the pull-down menu. (You can use the *group* attribute to map more than one group.)

Also see "Mapping Federated Groups" on page 377 under Federation Management.

User Mappings

See "Mapping Federated Users" on page 380 under Federation Management.

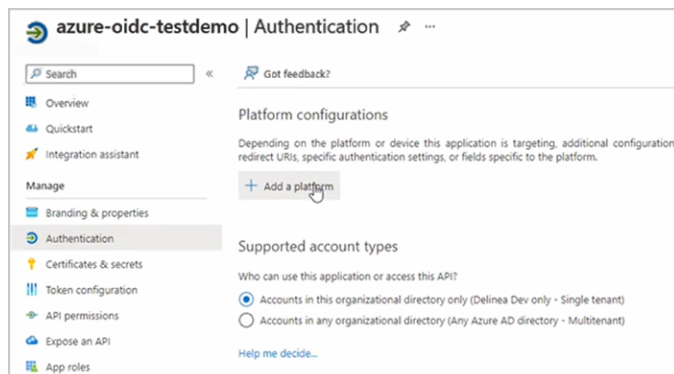
Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation. If you specify the Entra ID guest domain, then Entra guest users can also access the platform.

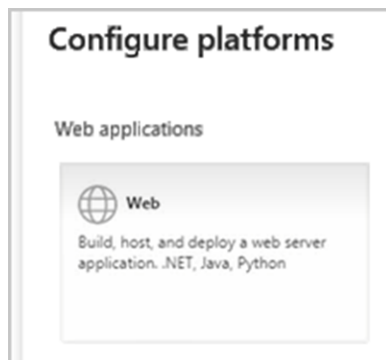
When all required fields are populated, click **Save**.

Add the Platform

1. On the **Entra App Registration** page, click **Authentication** and then **Add a platform**.



2. In the panel that opens on the right, click **Web**.

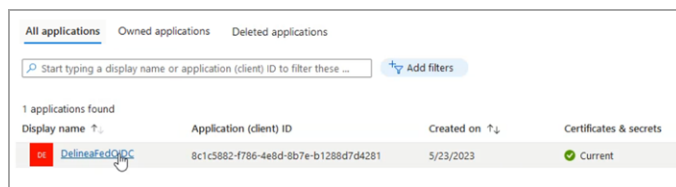


3. Under **Redirect URIs**, enter your Platform Callback URL from your provider page.
4. Click **Configure** at the bottom of the panel.

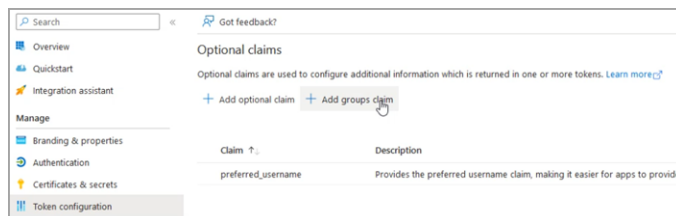
From Your Entra Application

1. Log in to your Microsoft Entra ID application and open to the Home page.
2. From the left navigation menu, click **App Registrations**.
3. Click the **All applications** tab.
4. Click the appropriate SAML or OIDC federation application created by your organization, for example:

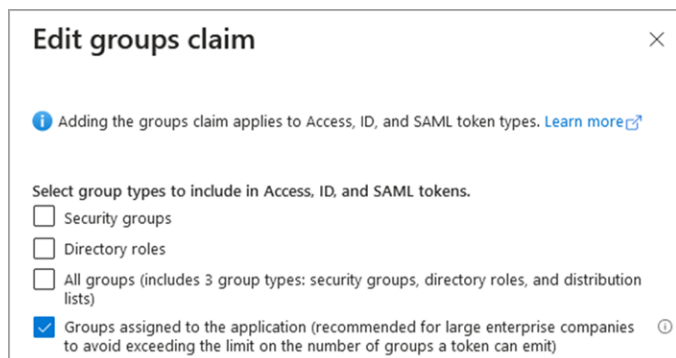
SAML and OIDC Federation



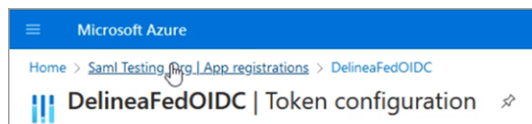
- From the left menu navigation, click **Token Configuration**.



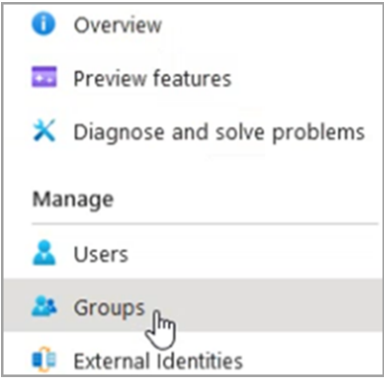
- Click **+ Add group claim**.
- From the panel that pops up named **Edit group claims**, select the group types to include. We strongly recommend selecting **Groups assigned to the application** to ensure that only the needed groups are sent to the platform.



- Click **Add** at the bottom.
- From the breadcrumb path at the top of the page, select the name of the Entra ID directory you're configuring, for example:



- Click **Groups** from the left navigation menu.



11. Select the group you are working with and copy the group's Object ID.

2 groups found

<input type="checkbox"/>	Name	Object Id	Group type	Membership type	Email	Source
<input type="checkbox"/>	postmanio	1fa239e9-2050-4e22-81a1-263b566d3691	Security	Assigned		Cloud
<input checked="" type="checkbox"/>	testgroup	51eeba12-4054-4638-bb4c-07736315dc4c	Security	Assigned		Cloud


From the Platform

1. Log out of the Platform.
2. Log back into the platform as a user who belongs to a platform group mapped to an Microsoft Entra ID group.
3. Click **Access** from the left navigation menu, then click **Groups** from the secondary menu.
4. Click a platform group that you've mapped to an Microsoft Entra ID group, where your user should appear.
5. Click the **Members** tab.
6. Verify that the user you logged in as, is a member of the platform group that you mapped to an Microsoft Entra ID group.

Integrating Entrust

This documentation is a detailed guide for setting up single sign-on (SSO) through Entrust, leveraging SAML 2.0 or OIDC.

The following procedures require copying and pasting information between Entrust and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

 **Note:** You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

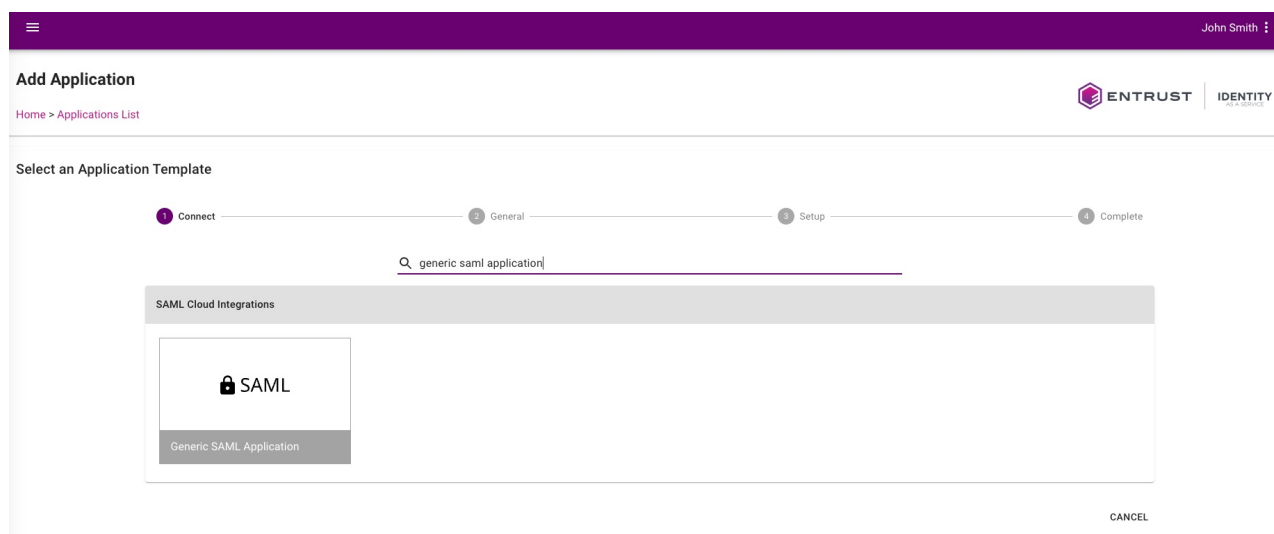
Prerequisites

On the Delinea Platform, you need to be an Admin with federation privileges.

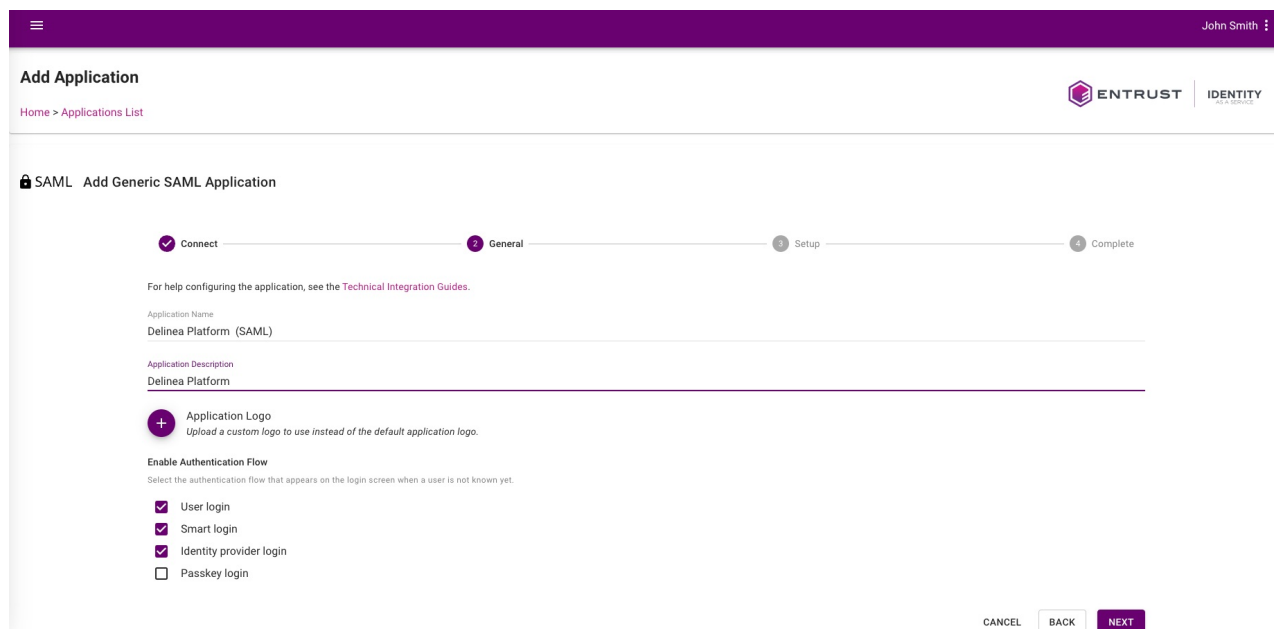
In Entrust, you need admin access to create SAML and OIDC applications.

Build an Entrust SAML Application

1. Log in to Entrust.
2. Navigate to Dashboard > **Applications** > **Applications List**.
3. Click **(+)** button to create a new application.
4. To narrow the list of SAML Cloud Integration, search for SAML, and select **Generic SAML Application**.



5. Provide a unique **Application Name**.
 - Optionally, provide a description and a logo for the application.
6. Click **Next**.



7. In the next section **General**, apply the following settings.

Entrust setting	Delinea Platform setting
Default Assertion Consumer Service URL	Platform callback URL https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer
Service Provider Entity ID (Issuer)	Customize certificate issuer sent to IDP Select this option, then copy and paste the value into the Service Provider Entity ID field of the Entrust SAML application.
Single Logout Service URL	Platform logout URL https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer

8. Continue updating the following application settings by selecting the value from the drop-down menu.

Entrust setting	Value
SAML NameID Attribute	Email
SAML Signing Certificate	`Default SAML Certificate` or you may specify another one
SAML NameID Encoding Format	EMAIL
SAML Signature Algorithm	SHA256

John Smith

Default Assertion Consumer Service URL *

https://example.delinea.app/identity-federation/saml/assertion-consumer

?

Service Provider Entity ID (issuer) *

https://example.delinea.app/identity-federation/sp/eda6207a-ef99-433f-be99-ae37d56cb596

?

Single Logout Service URL

https://example.delinea.app/identity-federation/saml/logout-consumer

?

SAML Username Parameter Name

?

SAML Session Timeout (minutes) *

5

?

SAML NameID Attribute *

Email

?

SAML NameID Encoding Format *

EMAIL

?

SAML Signing Certificate *

Default SAML Certificate

?

SAML Signature Algorithm *

SHA256

?

☒ Sign Complete SAML Response

☒ Enable Go Back Button

☒ Show Default Assertion Consumer Service URL in My Profile

☐ Encrypt SAML Assertion

☐ Override SAML Audience

9. Add SAML Attribute(s) with the key value pairs and click **Submit**.

Name	Value
DisplayName	<First Name> <Last Name>
EmailAddress	<Email>
NameIdentifier	<Unique User ID>
UserPrincipalName	<User Principal Name>

SAML Attribute(s)ADD

DisplayName

<First Name> <Last Name>

EmailAddress

<Email>

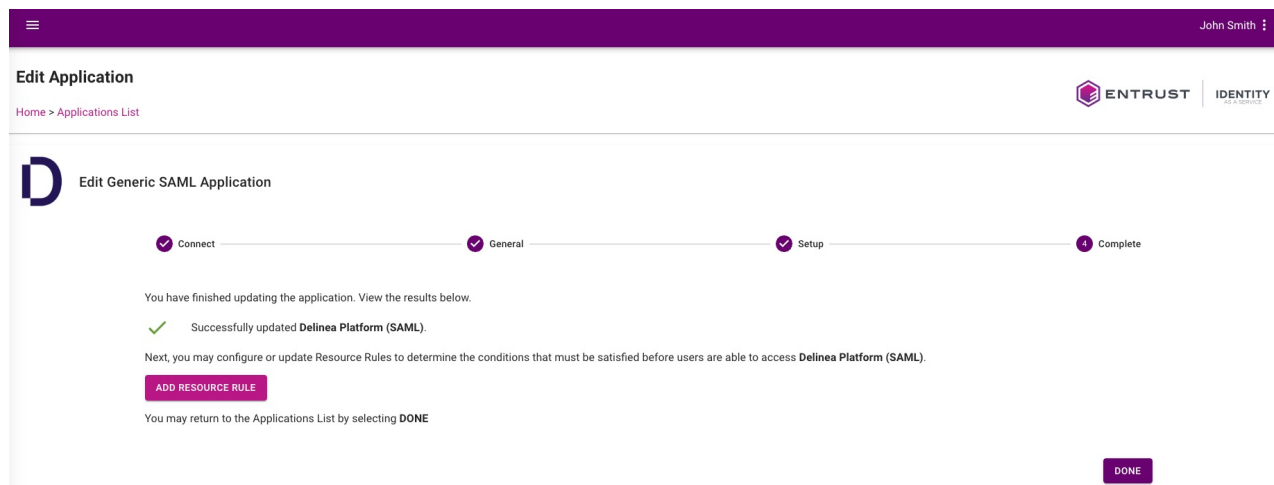
NameIdentifier

<Unique User ID>

UserPrincipalName

<User Principal Name>

10. Configure or update **Resource Rules** to specify the conditions users must meet to access the newly created application.



11. Click **Submit** when you're finished configuring your Resource Rules.
12. Next, navigate to the **Applications List**, find the SAML application, and download **SAML IDP Metadata**. This will be used when creating a SAML provider in the Delinea Platform.



Add the Provider to the Platform

1. Log in to the Delinea Platform.
2. Click **Settings** from the left navigation, then click **Federation Providers**.
3. Click **Add Provider**.
4. Select **SAML** from the drop-down menu. The **Add Provider** page opens.

Settings

In the **Settings** section, the first fields are automatically populated when you select the SAML provider configuration file and click **Apply**.

1. **SAML provider configuration:** Click **Select file**.
2. Navigate to and select the federation metadata XML file you downloaded. *Apply* appears above the right end of the SAML provider configuration field.
3. Click **Apply**. The words *Uploaded successfully* will appear next to SAML provider configuration, and the empty fields below will be auto-populated:
 - **Name:** Auto-generated from metadata
 - **Protocol:** SAML (auto-filled)
 - **Status:** Disabled
 - **Entity ID** [example: `https://sts.windows.net/808444af-4011-40d5-9b0a-a9a5c95f88e9/`]
 - **IDP Certificate:** Click **Select File**, then navigate to and select the Signing Certificate file you downloaded, to populate the following fields:
 - Signature
 - Algorithm
 - Thumbprint
 - Not valid before
 - Not valid after
 - Issuer
4. **IDP Login URL:** Paste in the **Login URL** copied from your new Entrust SAML application.
1. **IDP Logout URL:** Paste in the **Logout URL** copied from your new Entrust SAML application.
2. **Platform Callback URL:** `https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer`
Copy the Platform Callback URL and paste into the appropriate field in your new Entrust SAML application.
3. **Platform Logout URL:** `https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer`
4. **Status:** Select the box next to Enabled.

Advanced Settings

1. Under **Advanced Settings**, select **Customize certificate issuer sent to IdP**.
2. Copy the value provided and paste it into the **Service Provider Entity ID** field in the Entrust SAML application.

Also see ["Advanced Settings \(SAML only\)"](#) on page 374 under Federation Management.

Attribute Mappings

1. Update the Attribute Mappings as follows:

Source	Destination
EmailAddress	email
DisplayName	displayname
NameIdentifier	sub
UserPrincipalName	upn

Also see "Attribute Mappings" on page 376 under Federation Management.

Group Mappings

See "Mapping Federated Groups" on page 377 under Federation Management.

User Mappings

See "Mapping Federated Users" on page 380 under Federation Management.

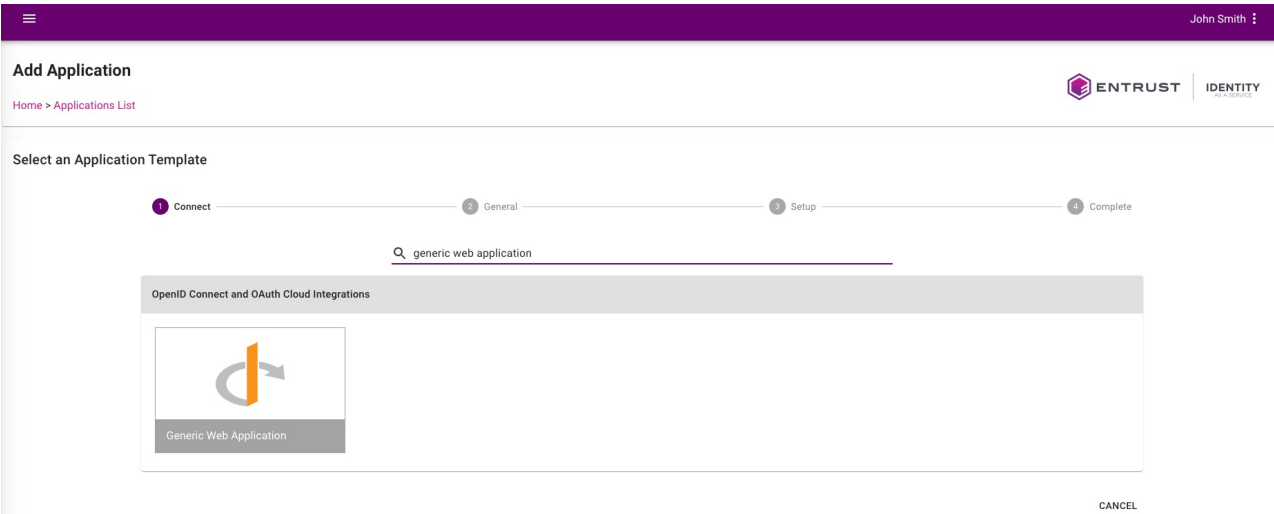
Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.
2. Optionally enable the Status of the provider.
3. When all required fields are populated, click **Add Provider**.

Build an Entrust OIDC Application

1. Log in to Entrust.
2. Navigate to Dashboard > **Applications** > **Applications List**.
3. Click (+) button to create a new application.

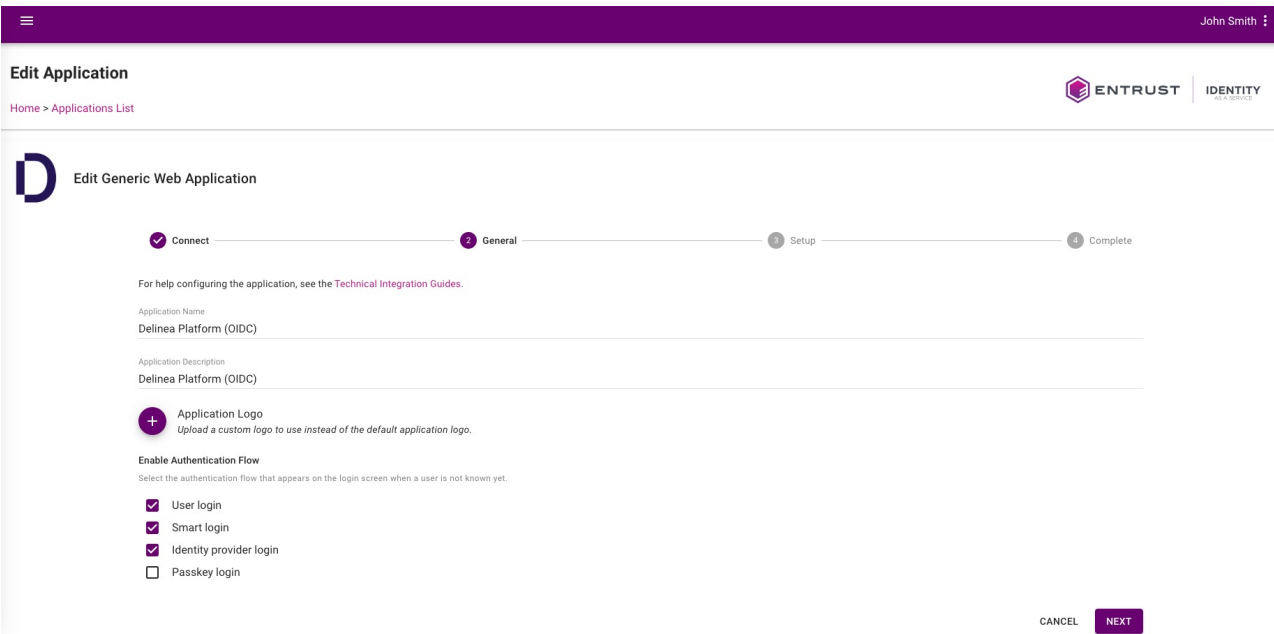
4. Search and select **Generic Web Application**.



5. Provide a unique **Application Name**.

- Optionally, provide a logo for the application, and a description.

6. Click **Next**.



7. Under the next section **General**, apply the following settings:

Entrust setting	Value
Client ID	Set automatically. Copy the Client ID into your Delinea Platform federation provider you will create later
Client Secret	Set automatically. Copy the Client ID into your Delinea Platform federation provider you will create later
Token/Revocation Endpoint Client Authentication Method	Client Secret Post
Subject ID Attribute	Email
OIDC Signing Certificate	`Default OIDC Certificate` or you may specify another one
Initiate Login URI	(Optional) - can be set to https://example.delinea.app
Login Redirect URI	Platform Callback URL (From the Delinea Platform) Follow steps 1-5 in the Add a Delinea Platform OIDC Provider section
Grant Types Supported	Authorization Code
Authorization Code PKCE Code Challenge Method	S256

John Smith

General Settings

Application Type
Web Application

Client ID
12345678901234567890

Client Secret *
.....

Token / Revocation Endpoint Client Authentication Method
Client Secret Post

Subject ID Attribute *
Email

OIDC Signing Certificate *
Default OIDC Certificate

Initiate Login URI (Optional)
https://example.delinea.app

Login Redirect URI(s) *
https://example.delinea.app/identity-federation/signin-oidc/1234567890

Logout Redirect URI(s)

Default Resource/Audience Request Value

Authentication Settings

Require Consent
☒ The user will be prompted for consent during authentication to this application.

Consent Message

Max Authentication Age (seconds)

Grant Types Supported *
Select the grant types that can be used. At least 1 must be selected.
Grant Type cannot be None or Implicit if Scope openid is not selected.
Grant Type cannot be Refresh Token if Grant Type Authorization Code is not selected.
☒ Authorization Code
☐ Client Credentials
☐ Implicit
☐ None (OIDC No Flow)
☐ Refresh Token (OIDC)

Authorization Code PKCE Code Challenge Method
S256

Include Authentication Time
☐ If enabled, include the authentication time with all ID tokens.


ID Token Signing Algorithm
RS256

ID Token Timeout (minutes)
5

8. Ensure that you select the following application support scopes:

- Your unique identifier
- Email address
- Telephone number (optional)

■ Profile information

 **Supported Scopes**

Select the scopes that may be requested in the authorization request.

☒

Your unique identifier
openid

☐

Address
address

▼

☒

Email address
email

▼

☒

Telephone number
phone

▼

☒

Profile information
profile

▼

9. Next, add or update the supported claims and ensure that they are always returned with ID Token.

Claim	Attribute Value	Always Return with ID Token
name	<First Name> <Last Name>	Yes
email	<Email>	Yes
nameidentifier	<Unique User ID>	Yes
upn	<User Principal Name>	Yes

★ Supported Claims

Select the claims that may be requested in the authorization request. This includes claims implied by the selected scopes.

+

Quick filter...

Claim	Attribute Value	Always Return with User Info	Always Return with ID Token	Actions
email	<Email>	No	Yes	<div><div></div><div></div></div>
name	<First Name> <Last Name>	No	Yes	<div><div></div><div></div></div>
nameidentifier	<Unique User ID>	No	Yes	<div><div></div><div></div></div>
upn	<User Principal Name>	No	Yes	<div><div></div><div></div></div>

Rows per page: 10 Total: 4

|<

Page 1 of 1

<

>

>|

* Required

10. Click **Submit**.
11. Configure or update **Resource Rules** to specify the conditions users must meet to access the newly created application.

John Smith

Edit Application

Home > Applications List

ENTRUST

IDENTITY

D

Edit Generic Web Application

✓ Connect

✓ General

✓ Setup

4 Complete

You have finished updating the application. View the results below.

✓

Successfully updated **Delinea Platform (OIDC)**.

Next, you may configure or update Resource Rules to determine the conditions that must be satisfied before users are able to access **Delinea Platform (OIDC)**.

ADD RESOURCE RULE

You may return to the Applications List by selecting **DONE**

DONE

12. Click **Submit** when you are finished configuring your Resource Rules.

Add the Provider to the Platform

1. Click **Settings** from the left navigation, then click **Federation Providers**.

2. Click **Add Provider**.

3. Select **OIDC** from the drop-down menu. The **Add Provider** page opens.

Delinea Delinea Platform

Administrator Guide

Page 426 of 846

Settings

Delinea Platform	Entrust
Endpoint URL	Issuer URL (e.g. https://example.us.trustedauth.com/api/oidc) This URL can typically be retrieved from the Issuer setting in the OIDC Configuration in Entrust.
Client ID	Client ID
Client Secret	Client Secret

1. **Name:** Enter a unique name.
2. **Status:** Select the box next to Enabled.
3. **Endpoint URL:** This URL is based on your IdP application's tenant ID.
4. **Client ID:** Paste in the Client ID from your new IdP OIDC application page.
5. **Client Secret:** Paste in the Client Secret from your new IdP OIDC application page.
6. **Prompt:** See Prompt for Re-authentication (OIDC only) under Federation Management.
7. **Platform Callback URL:** Copy the platform callback URL and paste it into the Redirect URIs field in your new IdP application.

Attribute Mappings

Source	Destination
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	upn
name	displayname
nameidentifier	sub

Group Mappings

See ["Mapping Federated Groups"](#) on page 377 under Federation Management.

User Mappings

See ["Mapping Federated Users"](#) on page 380 under Federation Management.

Domains

1. Click Add Domain and enter the domain from the email addresses of the users you are including in this federation.
2. Optionally enable the **Status** of the provider.
3. When all required fields are populated, click Add Provider.

Test Configuration

Before testing, make sure you address the following:

- Be sure that you have an Entrust user that you can use for testing.
- Make sure Entrust user has access to the application created.
- Navigate to your provider in platform and enable debugging.
- Launch an incognito window, navigate to the Delinea Platform and login with your Entrust user.


Known limitation(s)

- Entrust does not appear to recognize the login_hint provided by the Delinea Platform for SAML.
- With OIDC, users can be directed from the Entrust application portal to the Platform's login page, enabling an SP-initiated authorization flow.

Integrating Google

This documentation is a detailed guide for setting up single sign-on (SSO) through Google, leveraging SAML 2.0 or OIDC.

The SAML application is configured in Google Workspace, while the OIDC application is configured in Google Cloud. The Google Cloud OIDC flow does not natively support the `groups` claim. For details on supported claims, see [The Discovery document](#) from Google.

 **Note:** You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

 **Note:** If an IdP-initiated flow is required, SAML federation is recommended.

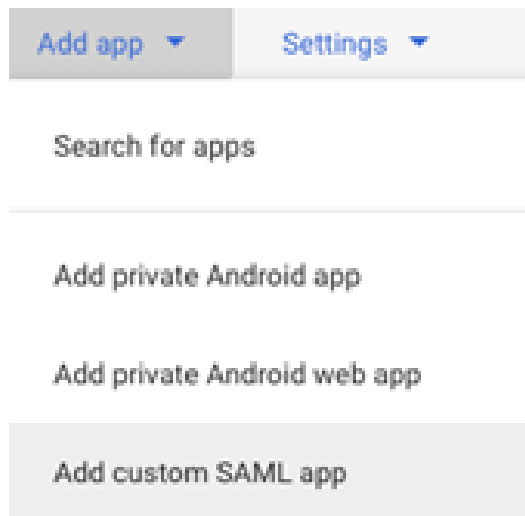
The following procedures require copying and pasting information between Google and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

Prerequisites

- On the Delinea Platform, you need to be an Admin with federation privileges.
- In Google Workspace (SAML app) and Google Cloud (OIDC app), you need an account with super administrator privileges.

Build a custom Google Workspace SAML app.

1. In the **Google Admin** console, go to **Apps > Web and mobile apps**.
2. Click **Add App > Add custom SAML app**.



3. On the **App details** screen, populate the **App name** and other (optional) fields:
 - a. **App name** (required)
 - b. **Description** (optional)
 - c. **App icon** (optional)
4. Click **Continue**.
5. On the **Google Identity Provider details** page, click **DOWNLOAD METADATA** to download the file, *GoogleIDPMetadata.xml*. The file contains the IdP metadata required by the Delinea Platform.
6. Click **Continue**.

Add the Provider to the Platform

1. Click **Settings** from the left navigation menu, then click **Federation Providers**.
2. Click **Add Provider**.
3. Select **SAML** from the drop-down menu. The **Add Provider** page opens.

Settings

In the **Settings** section, the fields are automatically populated when you upload the SAML provider configuration file and click **Apply**, as described below:

1. **SAML provider configuration:** Click **Select file**.
2. Navigate to and select the federation metadata XML file (e.g. GoogleIDPMetadata.xml) that you previously downloaded. The word, *Apply* will appear above the right end of the SAML provider configuration field.
3. Click **Apply**. The words *Uploaded successfully* will appear next to **SAML provider configuration**, and the fields below will be auto-populated:
 - Name: Auto-generated from metadata
 - Protocol: SAML (auto-filled)
 - Status: Disabled
 - Entity ID: [example: https://accounts.google.com/o/saml2?idpid=C02hflra4]
 - IDP Certificate:
 - Signature
 - Algorithm
 - Thumbprint
 - Not valid before
 - Not valid after
 - Issuer
 - IDP Login URL: (example: https://accounts.google.com/o/saml2/idp?idpid=C02hflra4)
 - IDP Logout URL: empty
 - Platform Callback URL: https://{HOSTNAME}/identity-federation/saml/assertion-consumer
 - Platform Logout URL: https://{HOSTNAME}/identity-federation/saml/logout-consumer
 - Status: disabled by default
4. (Optional) To rename federation, click **Edit**, update the **Name**, and click **Save**.

Advanced Settings

Under **Advanced Settings**, enable the option, **Customize certificate issuer sent to IdP** and copy the value. For details on other options, see [Advanced Settings \(SAML only\)](#) under [Federation Management](#).

Attribute Mappings

Under **Attribute Mappings**, configure user attributes as shown below. For details, see [Attribute Mappings](#) under [Federation Management](#).

SAML and OIDC Federation

Attribute Mappings

User attributes that are passed from the identity provider (IdP) to the Delinea Platform (SP) during the authentication and authorization process

SOURCE ↑	DESTINATION	
<input type="text" value="DisplayName"/>	<input type="text" value="displayname"/>	
<input type="text" value="EmailAddress"/>	email	Required Attribute
<input type="text" value="FirstName"/>	<input type="text" value="FirstName"/>	
<input type="text" value="LastName"/>	<input type="text" value="LastName"/>	
<input type="text" value="NameIdentifier"/>	sub	Required Attribute
<input type="text" value="UserPrincipalName"/>	upn	Required Attribute

[Add Attribute Mapping](#)

Group Mappings

(Optional) Under **Group Mappings**, configure the groups that will be included in the SAML response. For details, see [Mapping Federated Groups](#) under [Federation Management](#).

Example:

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME ↑	GROUP
Groups	federated_group	Test Group

To configure the IdP to send groups in the SAML response, refer to the "Update Google Workspace" on the next page section below.

User Mappings

See [Mapping Federated Users](#) under [Federation Management](#).

Domains

1. Navigate to the **Domains** section.
2. Click **Add Domain**.
3. Enter the domain from the email addresses of the users you are including in this federation.

Domains

Specify domains users may use as part of their login name

DOMAIN

No items found

[Add Domain](#)

[Cancel](#) [Save](#)

Update Google Workspace

Update the custom SAML app with the values from the Delinea platform.

1. In the **Service Provider Details** window, enter the following:
 - **ACS URL:** (the service provider's Assertion Consumer Service URL receives the SAML response). Enter the **Platform Callback URL** value from the platform.
 - **Entity ID:** (the globally unique name). Enter the **Customize certificate issuer sent to IDP** value from the platform.

2. Click **Continue**.
3. On the **Service provider details** page, update the **Attributes**.

4. (Optional) Enter group names that are relevant for this app. The **Google groups** name and the **App attribute** will be used to configure the Delinea Platform **Group Mappings** (to learn more about creating groups, see [Create a group in your organization](#) on Google Workspace Help Center):

SAML and OIDC Federation

- a. In the **Group membership (optional)** section, click **Search for a group**.
- b. Select a group.
- c. Add the App attribute, **Groups**.

Example:

The screenshot shows the 'Group membership (optional)' section. It includes a sub-header 'Group membership (optional)' and a descriptive text: 'Group membership information can be sent in the SAML response if the user belongs to any of the groups you add here.' Below this, there are two main sections: 'Google groups' and 'App attribute'. The 'Google groups' section has a search bar with 'federated_group' entered and a 'Search for a group' button. The 'App attribute' section has a dropdown menu with 'Groups' selected.

5. Click **Finish**.

Turn on Your SAML App

1. Select your SAML app.
2. Click **User access**.
3. Under **Service Status**, do one of the following:
 - To turn the service on or off for everyone:
 - Select **On for everyone** or **Off for everyone**
 - Click **SAVE**.
 - To turn the service on for a set of users across or within organizational units:
 - Update the **Groups** or **Organizational Units**.
 - For **Service status**, select the box next to **ON**.

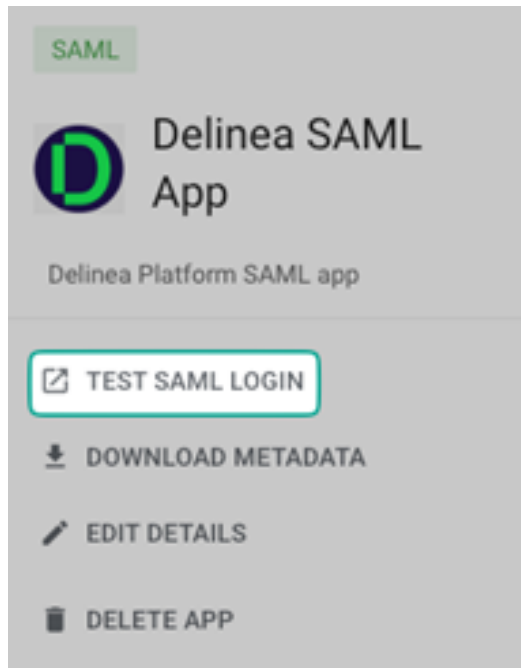
The screenshot shows a 'Service status' dialog box. It has a title bar 'Service status' with a close button. The main content area shows 'Service status' with a sub-label 'Not Set' and a checkbox that is checked, followed by the text 'ON'. At the bottom, there is a blue bar with the text '1 unsaved change' and two buttons: 'CANCEL' and 'SAVE'.

- Click **SAVE**.
4. Ensure that the user email addresses for signing in to the SAML app match the user email addresses for signing in to your Google domain.

Test Your SAML App

1. Select your SAML app.
2. Click **TEST SAML Login**

3. Log in.



4. If you are prompted to allow app access for a group or organizational unit that includes your admin account, click **ALLOW ACCESS**.

Can't test SAML login

To test SAML login, allow app access for a group or organizational unit that includes your admin account

[CANCEL](#) [ALLOW ACCESS](#)

Build a Custom Google OIDC App

1. In the **Google Cloud console**, navigate to **Credentials > CREATE PROJECT**.
2. Update the **Project name**, **Organization**, and **Location** fields as needed and click **Create**.
3. Select target users on the **OAuth consent** screen:
 - a. Select **User Type** (**Internal** or **External**).
 - b. Click **CREATE**.

4. Continue to configure details on the **OAuth consent** screen:
 - a. Update the **App name**, **User support email**, and **Developer contact information** fields as needed.
 - b. Click **SAVE AND CONTINUE**.
5. Configure **Scopes**.
 - a. Click **ADD OR REMOVE SCOPES**.
 - b. Select **.../auth/userinfo.email** scope.
 - c. Click **SAVE AND CONTINUE**.

OAuth consent screen — 2 **Scopes** — 3 Summary

Scopes express the permissions you request users to authorize for your app and allow your project to access specific types of private user data from their Google Account. [Learn more](#)

ADD OR REMOVE SCOPES

Your non-sensitive scopes

API ↑	Scope	User-facing description	
	.../auth/userinfo.email	See your primary Google Account email address	🗑️

🔒 Your sensitive scopes

Sensitive scopes are scopes that request access to private user data.

API ↑	Scope	User-facing description
No rows to display		

🔒 Your restricted scopes

Restricted scopes are scopes that request access to highly sensitive user data.

API ↑	Scope	User-facing description
No rows to display		

SAVE AND CONTINUE **CANCEL**

6. On the **Summary** page, edit as needed and click **BACK TO DASHBOARD**.
7. Create OAUTH 2.0 Credentials:
 - a. Navigate to **Credentials > CREATE CREDENTIALS**
 - b. Select **OAUTH client ID**.

- c. Select **Application type > Web application**.
 - i. Update the required fields as needed.
 - ii. Click **CREATE**.
 - iii. On the OAuth client create modal screen, copy and paste the **Client ID** and **Client secret** to a known location. These will be used to configure the Delinea Platform OIDC federation.
 - iv. In the **Authorized redirect URIs** section, click **ADD URI** and add the **Platform Callback URL** (in the next section, *Add the Provider to the Platform*, see "Settings" below).
 - v. Click **OK**.

Add the Provider to the Platform

1. Click **Settings** from the left navigation, then click **Federation Providers**.
2. Click **Add Provider**.
3. Select **OIDC** from the drop-down menu. The **Add Provider** page opens.

Settings

1. Update **Name**.
2. (Optional) Update **Status**.
3. Add **Endpoint URL**: `https://accounts.google.com/`
4. Update the **Client ID** with the Client ID value provided by Google.
5. Update the **Client secret** with the Client Secret value provided by Google.
6. (Optional) Update **Prompt**.
7. Copy and save the **Platform callback URL** value.


Attribute Mappings

Under **Attribute Mappings**, configure the user attributes as shown below. For details, see [Attribute Mappings](#) under [Federation Management](#).

Attribute Mappings		
User attributes that are passed from the identity provider (IdP) to the Delinea Platform (SP) during the authentication and authorization process		
SOURCE ↑	DESTINATION	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email	Required Attribute
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	upn	Required Attribute
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	sub	Required Attribute
name	displayname	

Group Mappings

See [Mapping Federated Groups](#) under [Federation Management](#).

 **Note:** The Google Cloud OIDC flow does not natively support the `groups` claim. For details on supported claims, see [The Discovery document](#) from Google. If group mapping is required, SAML federation is recommended.


User Mappings

See [Mapping Federated Users](#) under [Federation Management](#).

Integrating Okta

This documentation is a detailed guide for setting up single sign-on (SSO) through Okta, leveraging SAML 2.0 or OIDC.

The following procedures require copying and pasting information between Okta and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

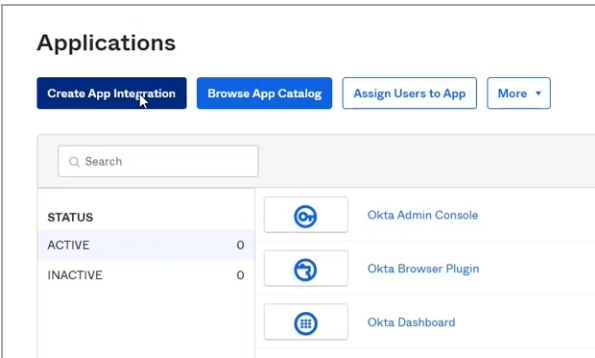
 **Note:** You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

Prerequisites

On the Delinea Platform, you need to be an Admin with federation privileges.

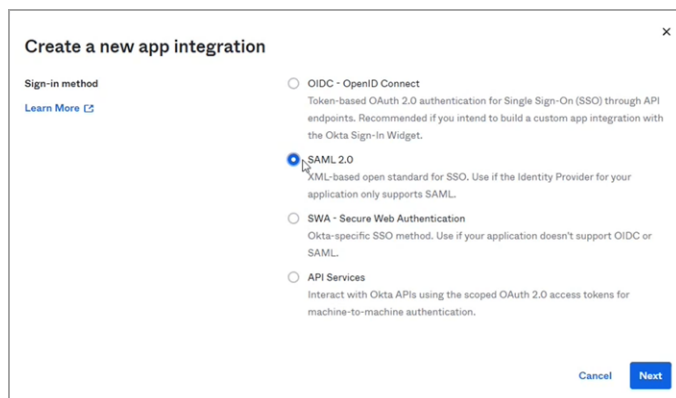
Build an Okta SAML Application

1. From the Okta left navigation menu, click **Applications**.
2. On the Applications page, click **Create App Integration**.



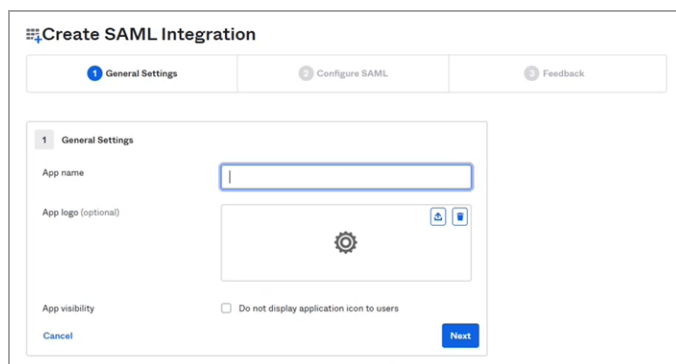
3. On the **Create a new app integration** page, select **SAML 2.0**.

SAML and OIDC Federation



A dialog box titled "Create a new app integration" with a close button (X) in the top right corner. It features a "Sign-in method" section with a "Learn More" link. Four radio buttons are listed: "OIDC - OpenID Connect" (described as token-based OAuth 2.0 authentication), "SAML 2.0" (selected, described as XML-based open standard for SSO), "SWA - Secure Web Authentication" (Okta-specific SSO method), and "API Services" (interact with Okta APIs using scoped OAuth 2.0 access tokens). "Cancel" and "Next" buttons are at the bottom right.

4. Click **Next**.
5. On the **Create SAML Integration** page under **General Settings**, enter a name into the **App name** field, such as `okta SAML`.



The "Create SAML Integration" page with three tabs: "General Settings" (active), "Configure SAML", and "Feedback". The "General Settings" section includes an "App name" text field, an "App logo (optional)" area with a gear icon and upload buttons, and an "App visibility" checkbox labeled "Do not display application icon to users". "Cancel" and "Next" buttons are at the bottom.

6. Click **Next**.
7. In the SAML Settings section next to **Single sign-on URL**, paste the following:
`https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer`
8. Replace [HOST-NAME] with the host name you selected when you created your tenant.

9. Next to **Audience URI (SP Entity ID)**, enter something intuitive, such as `Delinea_Federation`.
10. Scroll down to the **Attribute Statements** section.
11. Add three more blank attribute statements for a total of four.
12. Enter the following into the **Name** and **Value** fields of the four attribute statements:

Name	Value
EmailAddress	user.email
Name	user.displayName
nameidentifier	user.id
upn	user.login

13. Click **Next**.
14. On the **Create SAML Integration** page select, **I'm an Okta customer adding an internal app with Okta**
15. Click **Finish**
16. On your Okta new SAML application page, click the **Assignments** tab.

SAML and OIDC Federation

Back to Applications

1

Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

Submit your app for review

General
Sign On
Import
Assignments

Assign
Convert assignments

Search...

People

Filters
People
Groups

Person
Type

01101110
01101111
01100100
01100100
01100101
01101110
01100111

No users found

REPORTS
Current Assignments
Recent Unassignments

SELF SERVICE

You need to enable self service for org managed apps before you can use self service for this app.
Go to self service settings

Requests
Approval

Disabled
-

Edit

- Click the **Assign** drop-down and select **Assign to People** or **Assign to Groups**.
- In the next dialog box, click **Assign** next to the user(s) or group(s) you wish to assign to the federation.

Assign

Delinea Federation SAML to People

✕

Q Search...

John Doe

john.doe@saml-domain.com

Assign

Jane Smith

jane.smith@test-domain.com

Assign

Done

19. Click **Save and Go Back**.





Assign Delinea Federation SAML to People

User Name


Save and Go Back Cancel

20. Click **Done**.
21. On your Okta new SAML application page, click the **Sign-on** tab.



Delinea Federation SAML

[Active](#)[View Logs](#)[Monitor Imports](#)



Once you have a working SAML integration, submit it for Okta review to publish in the OAN.

General

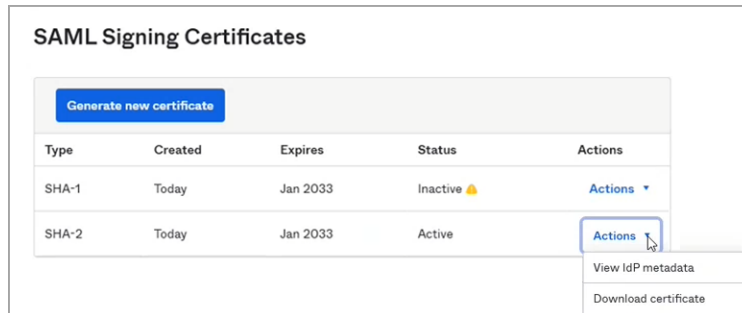
Sign On

Import


Assignments

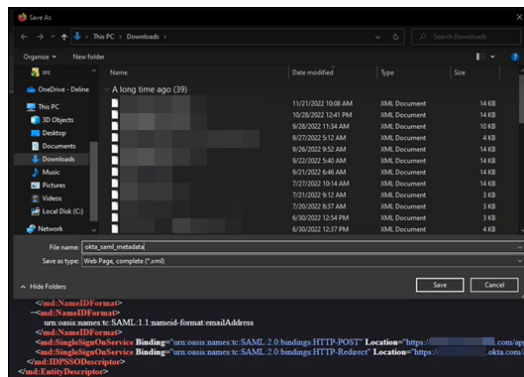
SAML and OIDC Federation

22. Scroll down to **SAML Signing Certificates**.
23. Click the **Actions** drop-down next to the Active certificate and select **Download certificate**.



24. Click the **Actions** drop-down next to the Active certificate and select **View IdP metadata**.
25. On the IdP metadata screen, right-click and choose **Save page as...** and select a name to save it as an xml file.

 **Note:** IdP Metadata is an XML-formatted document that contains configuration information necessary for Delinea Federation to authenticate against the identity provider and includes the required endpoint URLs, bindings, and certificates.



26. Navigate to **View SAML setup instructions** on the **Sign On** tab and download the X.509 certificate (okta.cert) as shown below.

3. X.509 Certificate:

-----BEGIN CERTIFICATE-----
MIIDqCCApCgAwIBAgIGA5Y32ctV0MA0GCSqGSIb3DQEBCwUAMIGUMQswCQYDVQGEwJVUzeETMBEGBA1UECAwKQ2FsaWZvcms1YTEuMBGGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MB1GA1UECwwlLNUHJvdmlkZXIzXjFATBGBNVBMMdGR1di0zMdC0MDc2MjEjMCBgBgGCSqGSIb3DQEBCwUAMIGUMQswCQYDVQGEwJVUzeETMBEGBA1UECAwKQ2FsaWZvcms1YTEuMBGGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEUJARYNAw5mb0Bva3RhLmNvbTAeFw0yNDAYMjkxOTU3NTdaFw0zNDAYMjg0OTU4NTdaMIGUMQswCQYDVQGEwJVUzeETMBEGBA1UECAwKQ2FsaWZvcms1YTEuMBGGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEUJARYNAw5mb0Bva3RhLmNvbTCCAS1wDQYJKoZIhvcNAQEBGggEADCCAQggEABJA4YYLl/ooowEUMd28ZuWz4f53VwWPNBg1oiKHE2G+vS29s01K6sunjgJ8teCT7Jz/hjYYPYLDb+esyIvWwHwfo15niCuFuUzu/ld4xsTaiq49mVTH5r1MR1WwvlyeNSdAMURJ91ltSugX1x/7t0tPwJ6LkLFGmlmmbfDXf3j3PvbybPq8HhV10kfiOPLB0JwkIY+H0/Wxup17x25K1I2cdQaGcwX2EKDAKIMJDUVAL/uisdEztLAKAJwEkb4n0eechrG95BEJt/W5V8eZ5SbzTvzxyrjEE0Jh1bdfJfR6XgAcf1FVJLpAc4QMqH1IT3r4deVqQ7hrWbYgY9CfAwEAATANBgkqhkiG9w0BAQsFAAOCAQEA
PCBn0Hc8JmCHLYA2P4mT7p4e+vCwWkdASU162pg09PfJrGGLZ2j7Hhwe/S47UnoAQ5FPmP7wWqOG
KS75BJfcgsCXBghqoB5KKKWFShw1b6H0V8tUX9KX4+vdDdghBx1meerCrKkG3ISxu/orbJsDH7cr
o3ydiuT61xARXnmkJU0vm9aV+T0t2rZrVaBqMscS80wprJCnwN7Hk18DC+XA82dcGTRURBZfgN
K1oY8Tb5Hb4uUoPgaxRLa9INQ1bzjdJz0+LunaSNisViUFPWU1CqInhz021glU76uD0EgC2TQ6
9a3r6zbXwE0wLIXqsR9HtQimpR0kDT181qCA==
-----END CERTIFICATE-----

[Download certificate](#)

27. Change the file extension to .pem. This will be your IDP certificate to download from the platform interface.

Add the Provider to the Platform

1. Click **Settings** from the left navigation, then click **Federation Providers**.
2. Click **Add Provider**.
3. Select **SAML** from the drop-down menu. The **Add Provider** page opens.

Settings

In the **Settings** section, the first fields are automatically populated when you select the SAML provider configuration file and click **Apply**.

1. **SAML provider configuration:** Click **Select file**.
2. Navigate to and select the federation metadata XML file you downloaded.
The word, ***Apply*** appears above the right end of the SAML provider configuration field.
3. Click **Apply**. The words *Uploaded successfully* will appear next to SAML provider configuration, and the empty fields below will be auto-populated:
 - **Name:** Auto-generated from metadata
 - **Protocol:** SAML (auto-filled)
 - **Status:** Disabled
 - **Entity ID** [example: <https://sts.windows.net/808444af-4011-40d5-9b0a-a9a5c95f88e9/>]

- **IDP Certificate:** Click **Select File**, then navigate to and select the Signing Certificate file you downloaded, to populate the following fields:
 - Signature
 - Algorithm
 - Thumbprint
 - Not valid before
 - Not valid after
 - Issuer
- 4. **IDP Login URL:** Paste in the Login URL from your Okta application by selecting the Sign on tab and copying the Sign On URL.
- 5. **IDP Logout URL:** Paste in the Logout URL from your Okta application.
- 6. **Platform Callback URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/assertion-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer)
Copy the Platform Callback URL to paste into the Sign-in redirect URIs field in your new Okta application.
- 7. **Prompt:** See "Prompt for Re-authentication (OIDC only)" on page 375 under Federation Management.
- 8. **Platform Logout URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/logout-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer)
- 9. **Status:** Select the box next to **Enabled**.

Advanced Settings

See "Advanced Settings (SAML only)" on page 374 under Federation Management.

Attribute Mappings

See "Attribute Mappings" on page 376 under Federation Management.

Group Mappings

1. Click the **General** tab.
2. Edit the SAML integration and click **Next** to configure the SAML settings.
3. Scroll down to **Group Attribute Statements**

Assertion Inline Hook	None (disabled)	
SAML Issuer ID	http://www.okta.com/\${org.externalKey}	
ATTRIBUTE STATEMENTS		
Name	Name Format	Value
nameidentifier	Unspecified	user.id
upn	Unspecified	user.login
EmailAddress	Unspecified	user.email
Name	Unspecified	user.displayName
GROUP ATTRIBUTE STATEMENTS		
Name	Name Format	Filter
groups	Unspecified	Matches regex: *

4. Set the following:

- Name:** groups
- Name format:** Unspecified
- Filter:** Matches regex: .*

This procedure affects all groups assigned to this application. If you want to apply it to a specific group or groups, change the filter as appropriate. More information is available from [the Okta website](#).

5. Click **Next** and **Save**.

Also see [Mapping Federated Groups](#) under Federation Management.

User Mappings

See [Mapping Federated Users](#) under Federation Management.

Domains

- Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.

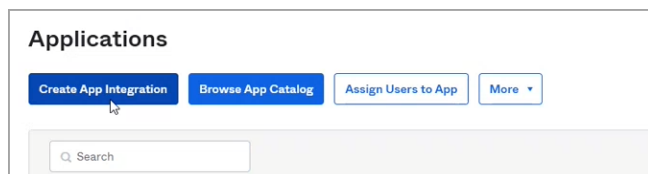
When all required fields are populated, click **Add Provider**.

Build an Okta OIDC Application

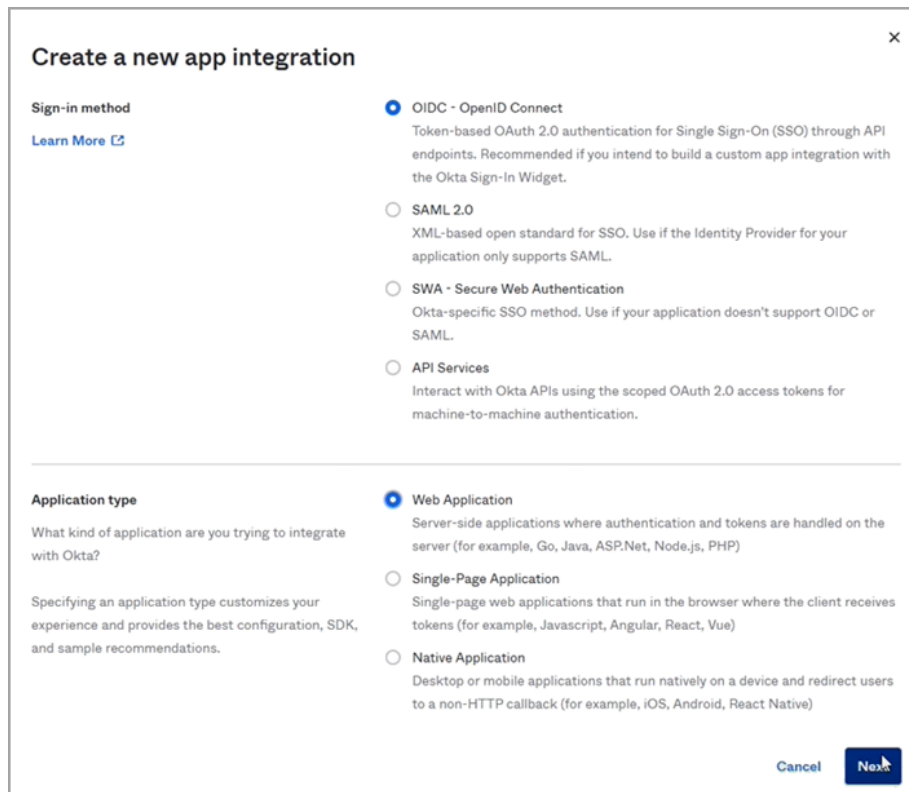


Note: The following procedure requires copying and pasting information between Okta and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

- From Okta, click **Applications** from the left navigation menu.
- Click **Create App Integration**.



3. In the **Create new app integration** dialog, next to **Sign-in method**, select **OIDC - OpenID Connect**.
4. Next to **Application Type**, select **Web Application**.
5. Click **Next**.



6. In the next dialog, next to **App integration name**, enter a name, such as `okta oidc`.
7. In the **Assignments** section, select one of the three choices.
8. Click **Save**.

Add the Provider to the Platform |

1. Click **Settings** from the left navigation, then click **Federation Providers**.
2. Click **Add Provider**.
3. Select **OIDC** from the drop-down menu. The **Add Provider** page opens.

Settings

1. **Name:** Enter a unique name.
2. **Status:** Select the box next to **Enabled**.
3. **Endpoint URL:** Paste in the Okta domain name copied from your Okta application page. You might need to add `https://` to the beginning.
4. **Client ID:** Paste in the Client ID copied from your Okta new OIDC application page.
5. **Client Secret:** Paste in the Client Secret copied from your Okta new OIDC application page.
6. **Platform Callback URL:** Copy the Callback URL. In your Okta new OIDC application, click **Add URI** and paste the copied callback URL into the **Sign-in redirect URIs** field.

Attribute Mappings

In the upn field, change the text to **preferred_username**.

Also see ["Attribute Mappings" on page 376](#) under Federation Management.

Group Mappings

From Your Okta Application

1. Log into the Okta Management site.
2. In the Admin Console, go to **Applications > Applications**.
3. Enter the name of the app integration in the **Search** field.
4. Click the **Assignments** tab.
5. Click **Assign** and select **Assign to Groups**.
6. Locate the group you want to assign the app integration to and click **Assign**.
7. Confirm the data is correct in the **Assign <application name> to Groups** dialog.
8. Click **Save and go back**. The Assigned button for the group is disabled to indicate the app integration is assigned to the group.
9. (Optional) Repeat to assign the app integration to additional groups.
10. Click **Done**.

From the Platform

1. Click **Add Group Mapping**.
 - **Attribute:** Enter **groups** (most other IdPs also use groups).
 - **Source Name:** Add the name of the appropriate group from Okta.
 - **Group:** Select a group from the pull-down menu (you can use the group attribute to map more than one group).

Also see [Mapping Federated Groups](#) under Federation Management.

User Mappings

See [Mapping Federated Users](#) under Federation Management.


Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.
2. Optionally enable the Status of the provider.
3. When all required fields are populated, click **Add Provider**.

Integrating OneLogin

This documentation is a detailed guide for setting up single sign-on (SSO) through OneLogin, leveraging SAML 2.0 or OIDC.

The following procedures require copying and pasting information between OneLogin and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

 **Note:** You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

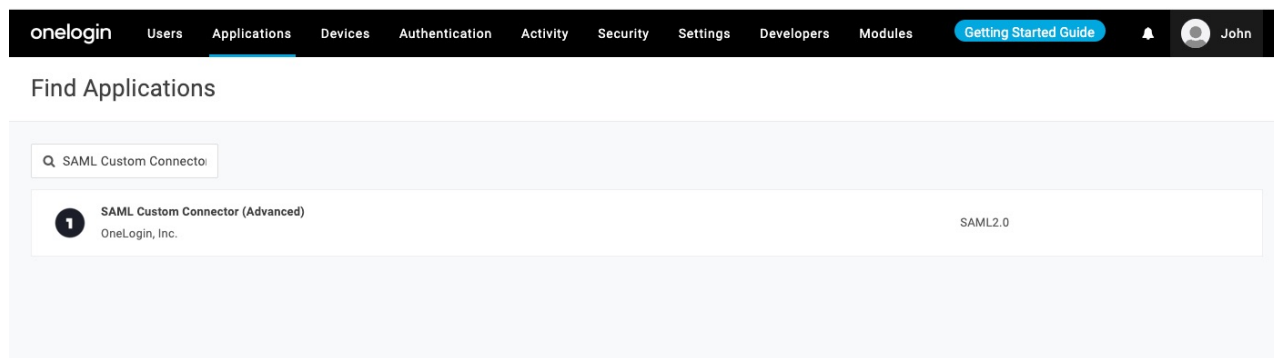
Prerequisites

On the Delinea Platform, you need to be an Admin with federation privileges.

In OneLogin, you need admin access to create a SAML and OIDC application.

Build a OneLogin SAML Application

1. Log in to the OneLogin Dashboard.
2. Navigate to **Applications > Add App**.
3. Search for SAML, and select **SAML Custom Connector (Advanced)**.



4. When prompted, update the **Display Name** of your application.

SAML and OIDC Federation

- Optionally, change **Visible in portal** setting
- Optionally, provide images for the application, and a description

5. Click **Save**.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules Getting Started Guide John

App Listing / Add SAML Custom Connector (Advanced) Cancel Save

Configuration

Portal

Display Name

Delinea Platform (SAML)

Visible in portal

✓

Rectangular Icon

Square Icon

Upload an icon with an aspect-ratio of 2.64:1 as either a transparent .PNG or .SVG

Upload a square icon at least 512x512px as either a transparent .PNG or .SVG

6. From the left navigation, select the **SSO**.

7. Update the **SAML Signature Algorithm** to **SHA-256**.

8. Click **Save**.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules Getting Started Guide John

Applications / SAML Custom Connector (Advanced) More Actions Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Enable SAML2.0

Sign on method

SAML2.0

X.509 Certificate

Standard Strength Certificate (2048-bit)

Change View Details

SAML Signature Algorithm

SHA-256

Issuer URL

https://app.onelogin.com/saml/metadata/1234567890-1234-1234-1234-1234567890

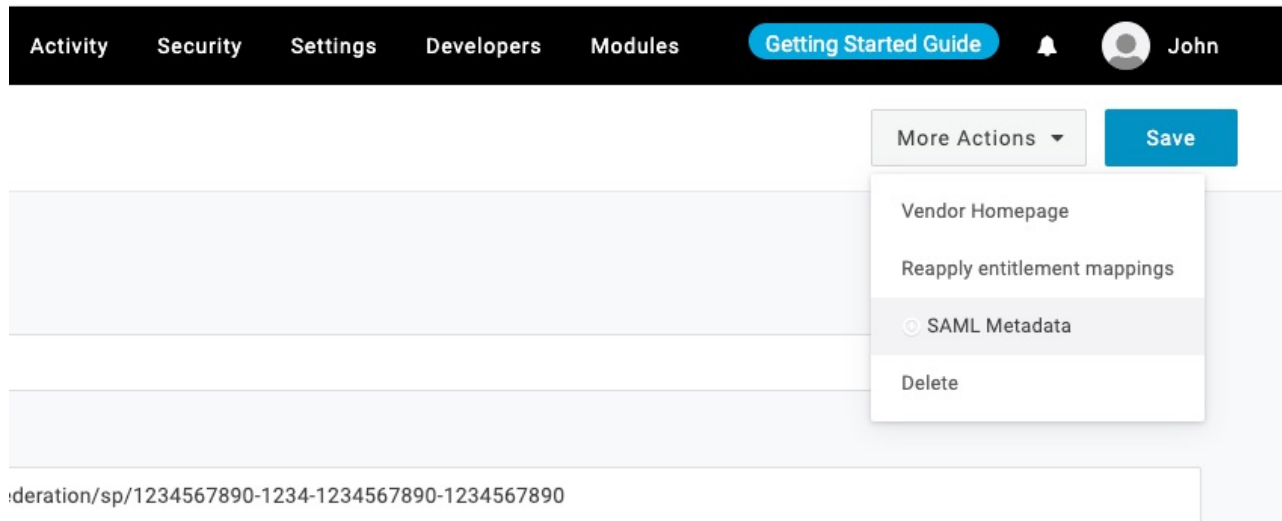
SAML 2.0 Endpoint (HTTP)

https://example.onelogin.com/trust/saml2/http-post/sso/1234567890-1234-1234-1234-1234567890

SLO Endpoint (HTTP)

https://example.onelogin.com/trust/saml2/http-redirect/slo/1234567890

9. Navigate to **More Actions** from the top right menu.
10. Download **SAML Metadata**.



11. Navigate to **Configuration** and fill out the below information.

OneLogin setting	Delinea Platform setting
Audience (Entity ID)	From Advanced Settings select and use the Customize certificate issuer sent to IDP value.
ACS (Consumer) URL Validator	Needs to be a valid RegEx of the ACS (Consumer) URL Platform callback URL. Modify the text in the example below according to the URL string of your platform tenant ^https:\\example\\.delinea\\.app\\identity-federation\\saml\\assertion-consumer\$
ACS (Consumer) URL	Platform callback URL https://{HOST-NAME}.delinea.app/identity-federation/saml/assertion-consumer

onelogin

UsersApplicationsDevicesAuthenticationActivitySecuritySettingsDevelopersModules

Getting Started Guide

John

Applications / SAML Custom Connector (Advanced)

More Actions

Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Application details

RelayState

Audience (EntityID)

https://example.delinea.app/identity-federation/sp/1234567890-1234-1234567890-1234567890

Recipient

ACS (Consumer) URL Validator*

*https://example.delinea.app/identity-federation/saml/assertion-consumer\$

*Required.

ACS (Consumer) URL*

https://example.delinea.app/identity-federation/saml/assertion-consumer

*Required

Single Logout URL

https://example.delinea.app/identity-federation/saml/logout-consumer

12. Click **Save**.
13. Go to **Parameters** and add the following custom attributes. For each field, make sure the **Include in SAML assertion** flag is selected.

SAML Custom Connector (Advanced) Field	Value
DisplayName	Name
EmailAddress	Email
NameIdentifier	OneLogin ID
UserPrincipalName	Username

SAML Custom Connector (Advanced) Field	Value
DisplayName	Name custom parameter
EmailAddress	Email custom parameter
NameID value	Email
NameIdentifier	OneLogin ID custom parameter
UserPrincipalName	Username custom parameter

Add the Provider to the Platform

1. Log in to the Delinea Platform.
2. Navigate to **Settings > Federation providers**.

Click **Add Provider** and select **SAML**. The **Add Provider** page opens,

Settings

In the **Settings** section, the first fields are automatically populated when you select the SAML provider configuration file and click **Apply**.

1. **SAML provider configuration:** Click **Select file**.
2. Navigate to and select the federation metadata XML file you downloaded. *Apply* appears above the right end of the SAML provider configuration field.
3. Click **Apply**. The words *Uploaded successfully* will appear next to SAML provider configuration, and the empty fields below will be auto-populated:
 - **Name:** Auto-generated from metadata
 - **Protocol:** SAML (auto-filled)
 - **Status:** Disabled
 - **Entity ID** [example: `https://sts.windows.net/808444af-4011-40d5-9b0a-a9a5c95f88e9/`]
 - **IDP Certificate:** Click **Select File**, then navigate to and select the Signing Certificate file you downloaded, to populate the following fields:
 - Signature
 - Algorithm
 - Thumbprint

SAML and OIDC Federation

- Not valid before
- Not valid after
- Issuer

1. **IDP Login URL:** Paste in the **Login URL** copied from your new OneLogin SAML application.
2. **IDP Logout URL:** Paste in the **Logout URL** copied from your new OneLogin SAML application.
3. **Platform Callback URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/assertion-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer)
Copy the Platform Callback URL and paste into the appropriate field in your new Entra application.
4. **Platform Logout URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/logout-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer)
5. **Status:** Select the box next to Enabled.

Advanced Settings

See ["Advanced Settings \(SAML only\)"](#) on page 374 under Federation Management.

Attribute Mappings

In the Attribute Mappings section, update these attributes as follows:

Source	Destination
DisplayName	displayname
EmailAddress	email
NameIdentifier	sub
UserPrincipalName	upn

Also see ["Attribute Mappings"](#) on page 376 under Federation Management.

Group Mappings

See [Mapping Federated Groups](#) under Federation Management.

User Mappings

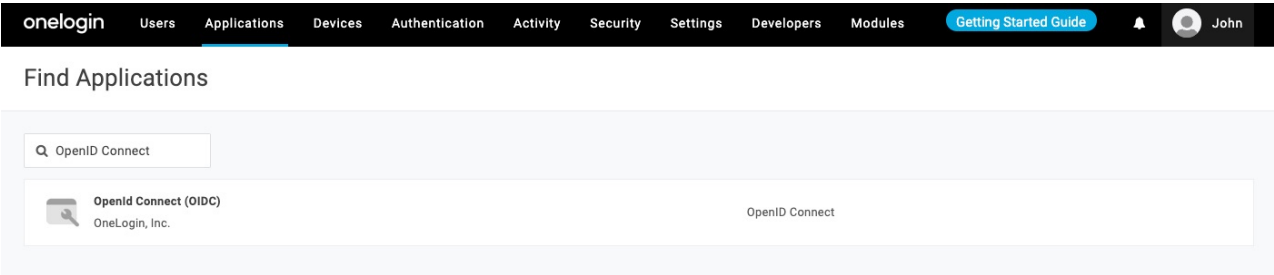
See [Mapping Federated Users](#) under Federation Management.

Domains

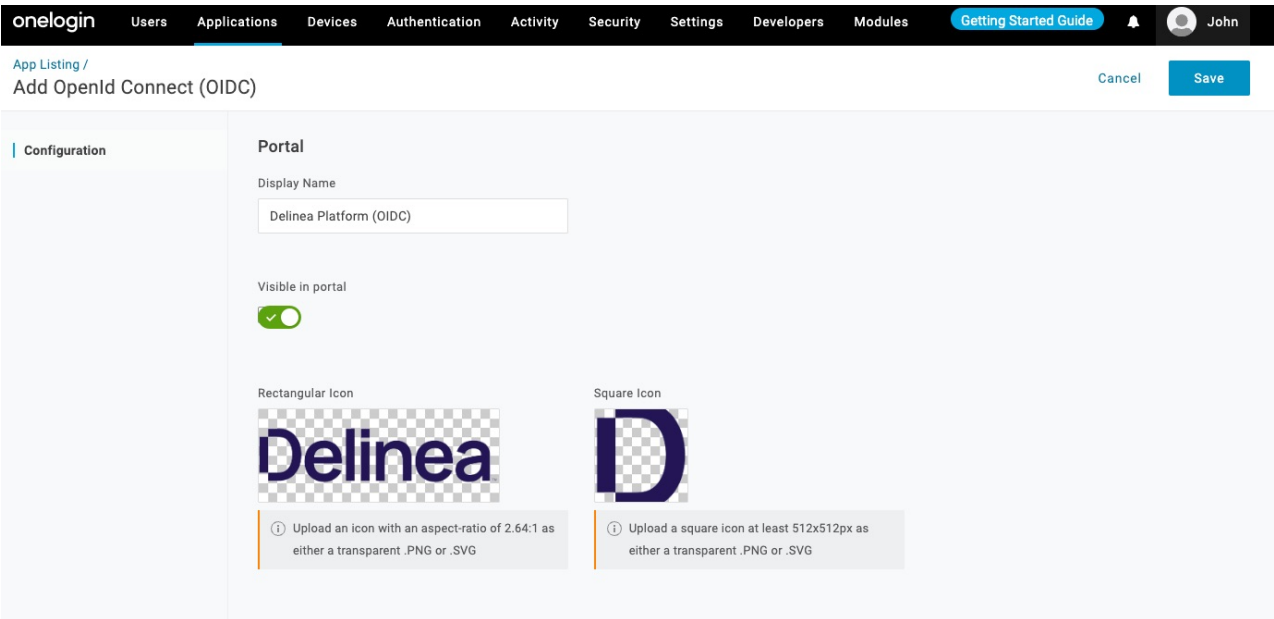
1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.
2. When all required fields are populated, click **Add Provider**.

Build a Onelogin OIDC Application

1. Log in to the OneLogin Dashboard.
2. Navigate to **Applications > Add App**.
3. Search for **OpenID Connect (OIDC)**.



4. When prompted, update the **Display Name** of your application.
5. Optionally, provide images for the application, and a description.
6. Click **Save**.



7. Continue with Configuration of the newly created application by updating the Redirect URI.

OneLogin	Delinea Platform
Login URL	Optional. You can set this to your tenant URL (e.g. https://example.delinea.app)

OneLogin	Delinea Platform
Redirect URL	Platform Callback URL. This value is automatically generated during the configuration of an OIDC Federation provider on the Delinea Platform. See Step 7 in the <i>Settings</i> section below.

onelogin

UsersApplicationsDevicesAuthenticationActivitySecuritySettingsDevelopersModulesGetting Started Guide

John

Applications / OpenId Connect (OIDC)

More Actions

Save

Info

Configuration

Parameters

Rules

SSO

Access

Users

Privileges

Setup

Application details

Login Url

Redirect URI's

https://example.delinea.app/identity-federation/signin-oidc/1234567890-1234-1234-1234567890

1

After the user is authenticated we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.
http://localhost is permitted for development purposes only and should not be used in production.

Post Logout Redirect URIs

https://example.delinea.app/

1

After the user is logged out by OIDC we only allow redirects back to entries on this comma (or new-line) separated list of urls, and HTTPS is required.
http://localhost is permitted for development purposes only and should not be used in production.

8. Next, navigate to **SSO**, and make note of the **Client ID**, **Client Secret**, and **Issuer URL** for use with your OIDC-enabled application. You would need this information when setting up OneLogin federation provider in the Delinea Platform.

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules [Getting Started Guide](#) John

Applications / OpenId Connect (OIDC) More Actions Save

[Info](#)
[Configuration](#)
[Parameters](#)
[Rules](#)
SSO
[Access](#)
[Users](#)

Enable OpenID Connect

Client ID

1234567890-1234-1234-1234-1234567890

Client Secret

[Show client secret](#) [Regenerate client secret](#)

Issuer URL

<https://example.onelogin.com/oidc/2> [Well-known Configuration](#)

9. Continue with the SSO settings.

Setting	Value
Application Type	Web
Token Endpoint	POST

onelogin Users Applications Devices Authentication Activity Security Settings Developers Modules [Getting Started Guide](#) John

Applications / OpenId Connect (OIDC) More Actions Save

[Info](#)
[Configuration](#)
[Parameters](#)
[Rules](#)
SSO
[Access](#)
[Users](#)
[Privileges](#)
[Setup](#)

Application Type

Web

Token Endpoint

Authentication Method

POST

Token Timeout settings

Access Token

Minutes

blank will default to 60 mins

Refresh Token

Minutes

blank will default to 30 days; password grant requires "offline_access" scope to return refresh token

10. Save the application settings.

11. Optionally, on the Users page, add users/groups who should have access to this application.

Add the Provider to the Platform

1. Click **Settings** from the left navigation, then click **Federation Providers**.
2. Click **Add Provider**.
3. Select **OIDC** from the drop-down menu. The **Add Provider** page opens.

Settings

1. **Name:** Enter a unique name.
2. **Status:** Select the box next to **Enabled**.
3. **Endpoint URL:** This URL is based on your OneLogin tenant ID.
4. **Client ID:** Paste in the Client ID from your new IdP OIDC application page.
5. **Client Secret:** Paste in the Client Secret from your new IdP OIDC application page.
6. **Prompt:** See "Prompt for Re-authentication (OIDC only)" on page 375 under Federation Management.
7. **Platform Callback URL:** Copy the platform callback URL and paste it into the Redirect URIs field in your new IdP application.

Attribute Mappings

Source	Destination
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	email
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	sub
name	displayname
preferred_username	upn

Group Mappings

See [Mapping Federated Groups](#) under Federation Management.

User Mappings

See [Mapping Federated Users](#) under Federation Management.

Domains

1. Click Add Domain and enter the domain from the email addresses of the users you are including in this federation.
2. Optionally enable the **Status** of the provider.
3. When all required fields are populated, click Add Provider.

Test Configuration

Before testing, make sure you address the following:

- Be sure that you have a OneLogin user that you can use for testing. If not, go to the Users tab on the OneLogin dashboard and add one.
- Make sure OneLogin user has access to the application created.
- Navigate to your provider in platform and enable debugging in the Federation console.
- Launch an incognito window, navigate to the Delinea Platform and login with your OneLogin user.

Known limitations

- OneLogin does not appear to recognize the login_hint provided by the Delinea Platform for both SAML and OIDC.
- When using OIDC and a Login URL is set in OneLogin (e.g., <https://example.delinea.app>), users can be redirected from the OneLogin application portal to the Platform's login page, enabling an SP-initiated authorization flow.

Integrating Ping Identity

This documentation is a detailed guide for setting up single sign-on (SSO) through PingOne, leveraging SAML 2.0 or OIDC.

The following procedures require copying and pasting information between PingOne and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.



Note: You do not need to configure both OIDC and SAML applications for your integration. Depending on your organization's infrastructure and preferences, you can choose either OIDC or SAML.

Prerequisites

- On the Delinea Platform, you need to be an Admin with federation privileges.
- In Ping Identity (PingOne), ensure that you have administrative privileges to manage application settings.

Build a Ping Identity SAML Application

1. Log in to your Ping Identity account.
2. From the main menu, select **Connections > Applications**.
3. On the Applications page, click the **+** button at the top of the page to add a new application.
4. Provide a name for your application and select **SAML Application**.

SAML and OIDC Federation

Add Application

×


Application Name *

Delinea

Description

Provide SSO for Delinea Platform

Icon





Max Size 1.0 MB


Application Type


Show Details


! Select an option below or view the [Application Catalog](#) to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

 SAML Application

 OIDC Web App

 Native

 Single-Page

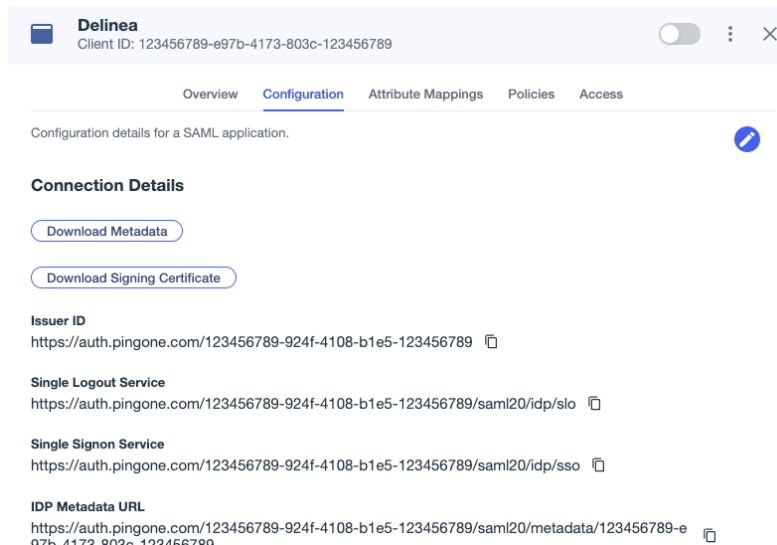
 Worker

Configure

Cancel

- Click **Configure**.
- In the SAML Configuration section, choose **Manually Enter**.
 - ACS URL**: `https://<tenant-name>.delinea.app/identity-federation/saml/assertion-consumer`
 - Entity ID**: Set it to none. We will revise this setting in the forthcoming instructions.
- Clicking **Configuration > Connection Details**
- Click **Download Metadata**.

9. Click **Download Signing Certificate**.



Add the Provider to the Platform

1. In a new browser tab, access the platform and log in.
2. Click **Settings** from the left navigation, then select **Federation Providers**.
3. Click **Add Provider**.
4. Select **SAML**. The **Add Provider** page opens.

Settings

In the **Settings** section, the first fields are automatically populated when you select the SAML provider configuration file and click **Apply**.

5. **SAML provider configuration**: Click **Select file**.
6. Navigate to and select the federation metadata XML file you downloaded.
The word, **Apply** appears as a clickable option above the right end of the SAML provider configuration field.
7. Click **Apply**. The words *Uploaded successfully* will appear next to SAML provider configuration, and the fields below will be auto-populated:
 - **Name**: Auto-generated from metadata
 - **Protocol**: SAML (auto-filled)
 - **Status**: Disabled
 - **Entity ID** [example: https://sts.windows.net/808444af-4011-40d5-9b0a-a9a5c95f88e9/]
 - **IDP Certificate**: Click **Select File**, then navigate to and select the Signing Certificate file you downloaded, to populate the following fields:

SAML and OIDC Federation

- Signature
 - Algorithm
 - Thumbprint
 - Not valid before
 - Not valid after
 - Issuer
8. **IDP Login URL:** Paste in the Login URL from your Ping Identity application.
 9. **IDP Logout URL:** Paste in the Logout URL from your Ping Identity application.
 10. **Platform Callback URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/assertion-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer)
Copy the Platform Callback URL to paste into the appropriate field in your Ping Identity application.
 11. **Platform Logout URL:** [https://\[HOST-NAME\].delinea.app/identity-federation/saml/logout-consumer](https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer)
 12. **Status:** Select the box next to **Enabled**.

Advanced Settings

1. **Customize certificate issuer sent to IDP:** Check the box to enable this setting. This setting overrides the default Certificate Issuer (also referred to as the *Entity ID*) information sent to the Identity Provider (IdP).
2. **Request Binding:** Update this setting to **HTTP-POST** for form-based. This setting controls the method for binding SAML authentication requests to the communication protocol.
3. **Sign Request:** Check the box to enable this setting. Upload your certificate (format supported pfx or p12). When enabled, this setting ensures that the SAML authentication request sent to the identity provider is digitally signed for added security.

Also see ["Advanced Settings \(SAML only\)"](#) on page 374 under Federation Management.

Attribute Mappings

Source | Destination

- EmailAddress | email*
- DisplayName | displayname
- saml_subject | sub*
- upn | upn*

Also see ["Attribute Mappings"](#) on page 376 under Federation Management.

Group Mappings

See [Mapping Federated Groups](#) under Federation Management.

User Mappings

See [Mapping Federated Users](#) under Federation Management.

Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.

When all required fields are populated, click **Add Provider**.

Post-configuration to Ping Identity Application

Update Entity ID

Adjust the Entity ID to match the customized issuer value previously chosen on the platform.

Attribute Mappings

1. Go to the **Attribute Mappings** tab.
2. Add or modify the parameters as shown below:
 - saml_subject | User ID (mark as required)
 - EmailAddress | Email Address (mark as required)
 - displayname | Name (Formatted)
 - upn | Username (mark as required)

The screenshot shows the Delinea configuration interface for a PingOne application. At the top, the application name 'Delinea' and its Client ID '1234567890-e97b-4173-803c-1234567890' are displayed. Below this is a navigation bar with tabs: Overview, Configuration, Attribute Mappings (selected), Policies, and Access. A message states: 'These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See [Mapping attributes](#).' Below this is a warning box: 'If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.' The main section shows a table of attribute mappings between Delinea and PingOne:


Delinea	PingOne	Required
saml_subject	User ID	Required
EmailAddress	Email Address	Required
displayname	Formatted	
upn	Username	Required

3. Click **Save**.

Activate the Application

Activate the application by engaging the toggle button in the top-right corner.

SAML and OIDC Federation

 **Delinea**
Client ID: 1234567890-e97b-4173-803c-1234567890

☒ ⋮ ✕

Overview

Configuration


Attribute Mappings

Policies

Access

Signing Algorithm
RSA_SHA256

Encryption
Disabled

Entity ID
<https://pmplatform.secureplatform.io/identity-federation/sp/1234567890-012b-1234567890> 

SLO Endpoint
Not Specified

Subject NameId Format
Not Specified


Assertion Validity Duration
300 seconds

Target Application URL
Not Specified

Enforce Signed AuthnRequest
Disabled

Verification Certificates
[example.com](#)
Valid 08-23 to 08-24

Select Policy based on RequestedAuthnContext
Disabled

Environment ID
1234567890-924f-4108-b1e5-1234567890 

Map Ping Identity and Platform Groups

From Your Ping Identity Application

Users can be automatically assigned to groups on the platform by sending their group memberships from PingOne.

1. Go to the PingOne application > **Attribute Mappings**.
2. Click **Edit**.
3. Add a new attribute by clicking the **+ Add** button.
The new attribute should be as follows:
groups | Group Names

SAML and OIDC Federation

Delinea	PingOne
saml_subject	User ID Required
EmailAddress	Email Address Required
displayname	Formatted
groups	Group Names
upn	Username Required

4. Click **Save**.

From the Platform

1. Click **Settings** from the left navigation, then select **Federation Providers**.
2. Click the Ping One provider.
3. Click **Edit**.
4. Click **Add Group Mapping**.
 - **Attribute:** groups
 - **Source Name:** Use the PingOne group.
 - **Group:** Select the Delinea group.

Group Mappings		
Map users into groups according to specified Group attribute values.		
<div>Edit</div>		
1 item		
<div><div></div><div></div></div>		
ATTRIBUTE	SOURCE NAME	GROUP
groups	Testgroup	System Administrator

Test Connection

1. On the Delinea Platform, go to the Debug Log tab for the provider.
2. Select **Start Debug Log**.
3. Open a new web browser tab in incognito mode and open the Delinea Platform.
4. Try logging in using a federated account.
5. Review the results in the original tab.



Note: For additional details regarding troubleshooting federated log-ins, refer to *Debugging the Federation Log* on the "Managing Federations" on page 373 page.

Settings

Mappings

Outbound Metadata

Debug Log

TIMESTAMP	EMAIL	UPN	INCOMING ATTRIBUTES	MAPPED CUSTOM ATTRIBU...	MAPPED GROUPS	MISSING REQUIRED ATTRIB...	ADDITIONAL DETAILS
9/10/2023 12:45 PM	testpingone@example.com	testpingone@example.com	5	4	1	0	User access granted

Incoming Attributes

These are the attributes received from the external Identity Provider (IDP). They follow a specific format. Each attribute consists of a key-value pair, where the key represents the attribute name and the value represents its corresponding value.

- **DisplayName** : Test User
- **EmailAddress** : testpingone@example.com
- **groups** : Testgroup
- **saml_subject** : e20f5ad9-be10-49b1-9195-23ca10fc0ab4
- **upn** : testpingone@example.com

Mapped Custom Attributes

After undergoing attribute mapping transformation, the attributes are mapped to a standardized format. Each mapped attribute follows a key-value pair structure, where the key represents the custom destination attribute name and the value represents its corresponding value.

- **displayname** : Test User
- **email** : testpingone@example.com
- **sub** : e20f5ad9-be10-49b1-9195-23ca10fc0ab4
- **upn** : testpingone@example.com

Mapped Groups

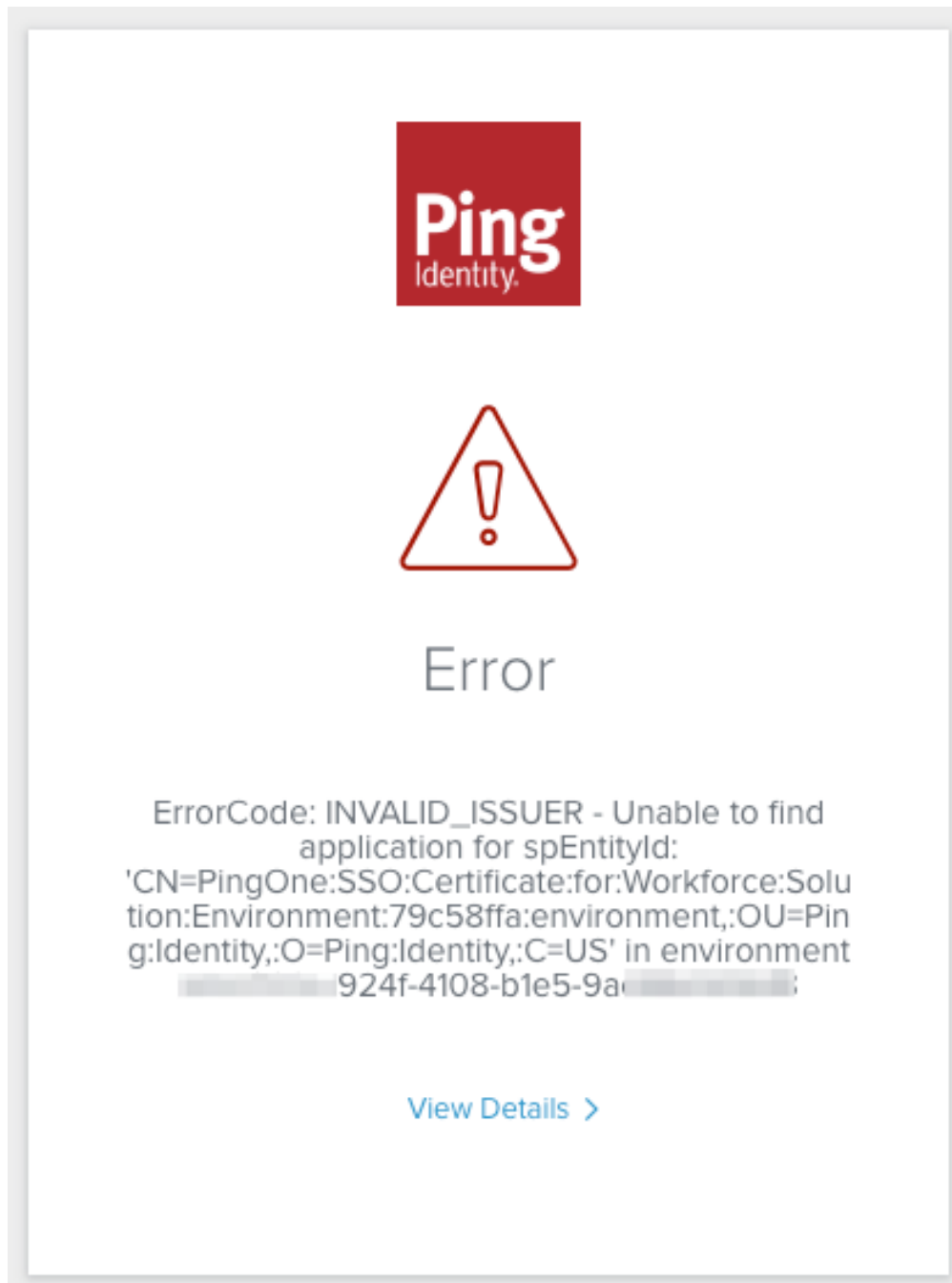
After undergoing group mapping transformation, the group values are mapped to a standardized format: The group from the IDP (source) : corresponding mapped Delinea group (destination)

- **Testgroup** : System Administrator

Troubleshooting

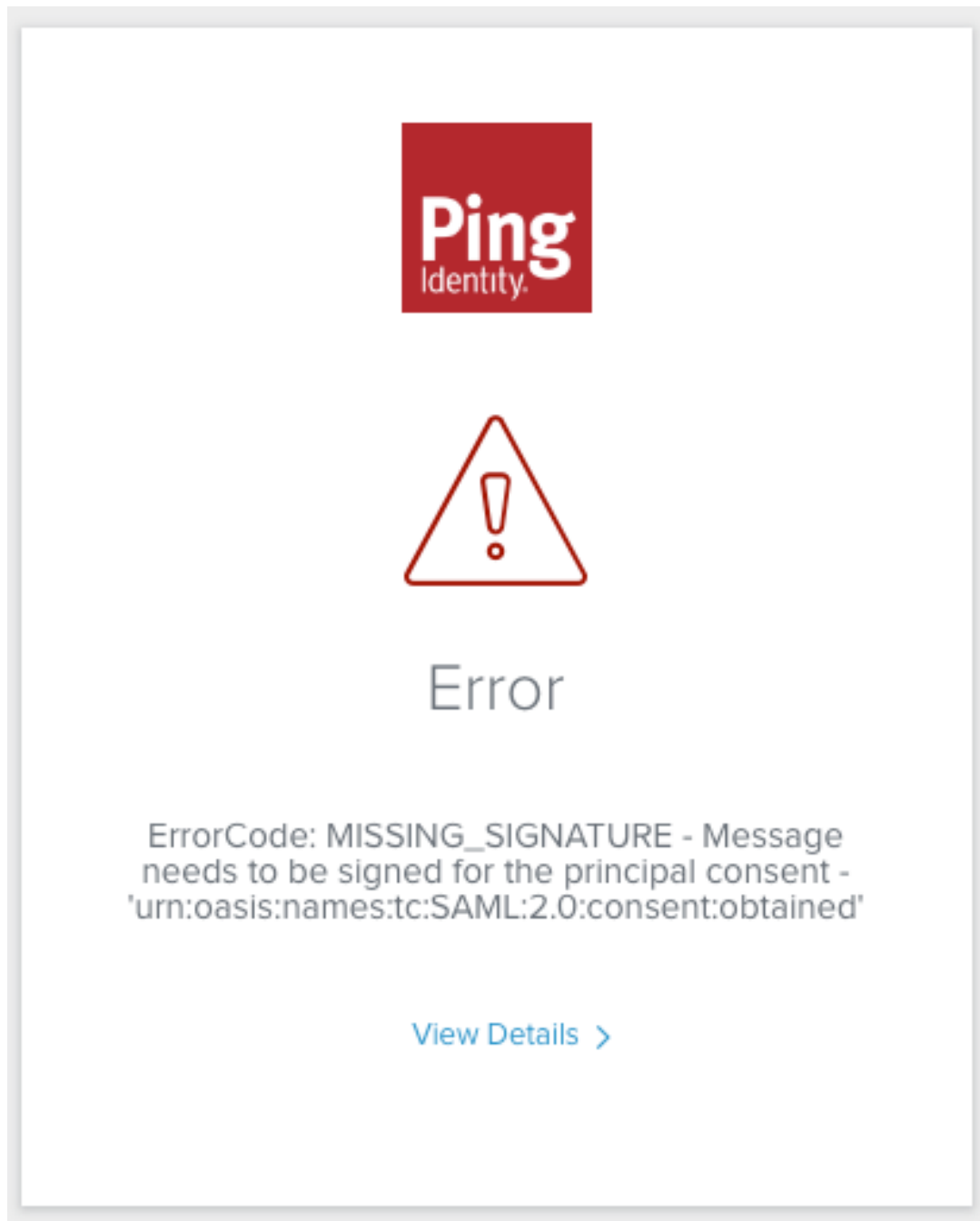
ErrorCode: Invalid Issuer - Unable to find application for spEntityId

Solution: This error commonly occurs when the Entity ID is either not configured or when there is a discrepancy for the Entity ID between the IdP and SP settings.



ErrorCode: MISSING_SIGNATURE - Message needs to be signed for the principal consent

Solution: Typically, this error arises when the sign request certificate on the platform is not set up or when the request binding is not set to HTTP-POST.



Build a Ping Identity OIDC Application

1. Log in to your Ping Identity account.
2. From the main menu, select **Connections > Applications**.
3. On the Applications page, click the **+** button at the top of the page to add a new application.
4. Provide a name and description for your application and select **OIDC Web App**.

SAML and OIDC Federation

Add Application [X]

Application Name *
Delinea

Description
PingOne OIDC set up with Delinea Platform

Icon
[Icon Placeholder]
Max Size 1.0 MB

Application Type [Show Details](#)

! Select an option below or view the [Application Catalog](#) to use a templated integration. If you can't find what you need in the catalog, consider SAML or OIDC to get started.

☐ SAML Application ☒ **OIDC Web App** ☐ Native

☐ Single-Page ☐ Worker

Save Cancel

5. Click **Save**.

Configure the Application on Ping Identity

1. Select the **Configuration** tab.
2. Click the **Edit** (pen) button.
3. Change the token endpoint authentication method (Token Auth Method) to: **Client Secret Post**.

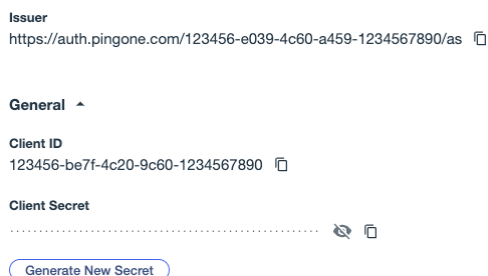
Add the Provider to the Platform

1. In a new browser tab, access the Platform and log in.
2. Click **Settings** from the left navigation, then select **Federation Providers**.
3. Click **Add Provider**.
4. Select **OIDC** from the drop-down menu. The **Add Provider** page opens.

Settings

1. **Name:** Enter a unique name.
2. **Status:** Check the box next to **Enabled**.

3. **Endpoint URL:** Locate the Issuer URL listed for your application under **PingOne > Configuration > URLs** and select the metadata file previously downloaded from PingOne.
4. **Client ID:** copy and paste in the client ID from your PingOne application as shown below:



5. **Client Secret:** Copy and paste in the client secret from your PingOne application.
6. **Prompt:** See "Prompt for Re-authentication (OIDC only)" on page 375 under Federation Management.
7. **Platform callback URL:** Copy the Callback URL. Add the platform's callback URL to the Redirect URIs setting in Ping Identity.

Attribute Mappings

Modify the attributes to align with the following:

Source | Destination

- EmailAddress | email*
- DisplayName | displayname
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier | sub*
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn | upn*

Group Mappings

Follow the steps under "Map Ping Identity and Platform Groups" on page 462 on this page.

Also see [Mapping Federated Groups](#) under Federation Management.

User Mappings

See [Mapping Federated Users](#) under Federation Management.

Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.

When all required fields are populated, click **Add Provider**.

Post-configuration to Ping Identity

Update Redirect URIs

Add the platform's callback URL to the Redirect URIs setting in Ping Identity.

Response Type
Code, ID Token, Access Token

Grant Type
Client Credentials, Implicit, Authorization Code

PKCE Enforcement
OPTIONAL

Redirect URIs
https://example.delinea.app/identity-federation/signin-oidc/123456-e225-48d7-96b4-1234567890

Allow Redirect URI patterns
False

Signoff URLs
None Specified

Token Auth Method
Client Secret Post

Require Pushed Authorization Request
Not Selected

Attribute Mappings

1. Go to the **Attribute Mappings** tab.
2. Add or modify the parameters as shown below:
 - sub | User ID (mark as required)
 - DisplayName | Name (Formatted)
 - EmailAddress | Email Address (mark as required)
 - upn | Username (mark as required)

SAML and OIDC Federation

OverviewConfigurationResourcesPoliciesAttribute MappingsAccess

These mappings associate PingOne user attributes to SAML or OIDC attributes in the application. See [Mapping attributes](#).

If this Application is accessible by users from more than one External IdP, it is recommended that you map the Identity Provider ID attribute so the Application can distinguish users by their IdP.

Custom Attributes ^

These attributes are currently mapped to the application. Customize them to meet your needs.

Attributes	PingOne Mappings		Scopes	
sub	User ID	?	openid	Required
DisplayName	Formatted	?	openid	
EmailAddress	Email Address	?	openid	Required
upn	Username	?	openid	Required

Inherited Global Attributes v

These global attributes are currently mapped to the application and specified in [Mapped attributes](#).

No Inherited Global Attributes

Enabling the Application

Activate the application by enabling the toggle button in the top-right corner.

Delinea

Client ID: 123456-be7f-4c20-9c60-1234567890

OverviewConfigurationResourcesPoliciesAttribute MappingsAccess

Configuration details for an OIDC application.

URLs v

General ^

Client ID
123456-be7f-4c20-9c60-1234567890

Client Secret
.....

Generate New Secret

Environment ID
123456-e039-4c60-a459-1234567890

Test Connection

Follow the steps under "Test Connection" on page 463 in the SAML portion of this document.

Integrating RSA SecurID

RSA offers automated identity intelligence, authentication, access, governance, and lifecycle capabilities to safeguard against cybersecurity risks for the most sensitive organizations. RSA SecurID is a technology that provides multi-factor authentication (MFA) to protect network resources.

The following RSA SecurID integrations are available:

[Integrating RSA ID Plus Cloud Authentication Service using My Page SSO with the Delinea Platform](#)

[Integrating RSA ID Plus Cloud Authentication Service using Relying Party with the Delinea Platform](#)

Troubleshooting Federated Group Mapping

Platform Group Sync Overwrites Secret Server Groups Every Four Hours

- The Secret Server users are stripped of their group memberships.
- The administrator might receive the error message, *No internal user found for mapping the external user.*

The customers affected are Secret Server customers who opted in to the Delinea Platform, with federated directory users on the platform and the following set up and working properly:

- Active Directory Synchronization
- The Delinea Connector
- Group Mapping

Resolution:

1. **From the Platform interface, remove all federated users from the platform.**
 - a. Click **Access** from the left navigation menu, then click **Users**.
 - b. Select the box next to a user from a federated directory.
 - c. Click **Delete** at the top right of the page.
 - d. Repeat steps b and c until all federated users are deleted.
2. **Ensure that your federation providers have their user mapping option set to "Required" with the option to 'Create local user if unable to map' enabled.**
 - a. Click **Settings** from the left navigation menu, then click **Federation providers**.
 - b. Click the name of a federation provider.
 - c. On the **Settings** tab, scroll down to **User Mappings**.

User Mappings

By default, when a federated user attempts to login, login will fail if a user with the same username exists in another directory service. When this feature is enabled, rather than failing login, the user of the federation will authenticate as the matching user of another directory service.

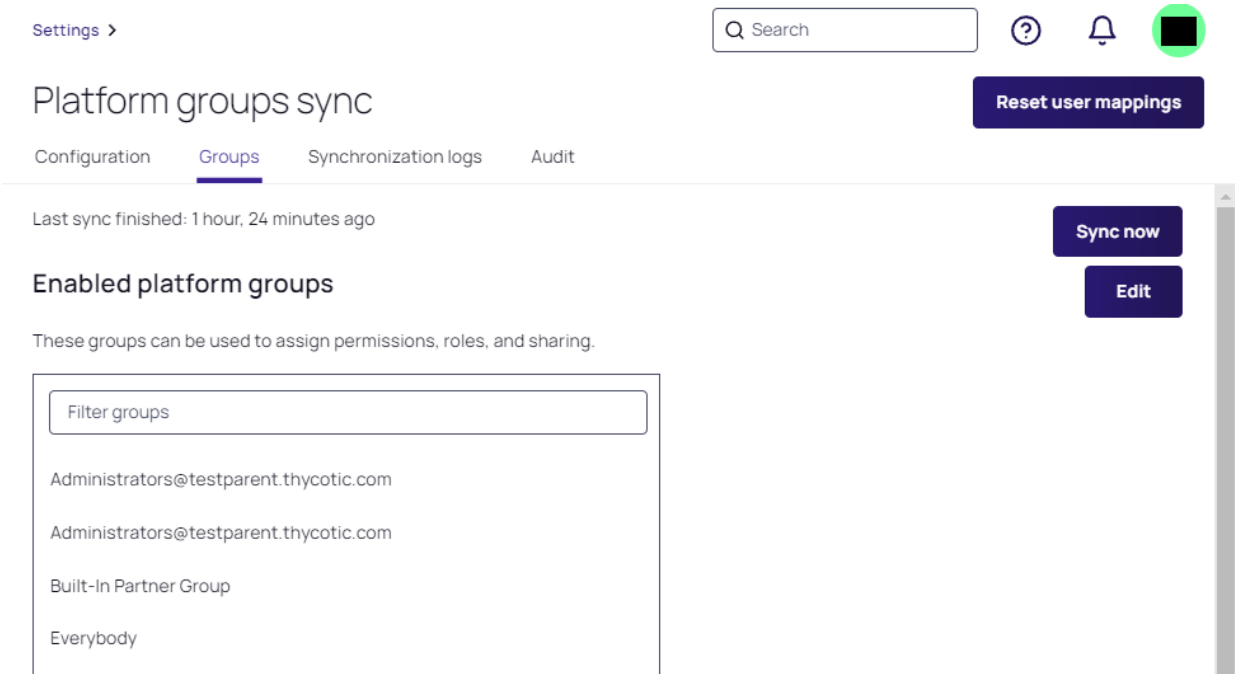
Map federated user to existing directory user

Required

☒ Create local user if unable to map

☐ Update local users with federated user attributes

- d. Next to **Map federated user to existing directory user**, select **Required** from the drop-down menu.
 - e. Select **Create local user if unable to map**.
 - f. Click **Save**.
3. From the Secret Server interface, reset user mappings
- a. Click **Settings** from the left navigation menu, then click **Platform groups sync**.



- b. On the Groups tab, click **Reset user mappings**.
- The next time those federated users log on to the platform, they should experience no more group issues.

Multi-Factor Authentication

The Delinea Platform provides cloud-based, flexible multi-factor authentication (MFA) as powerful as many retail MFA products and services. It is strongly recommended that all administrators and business users on the platform be required to use multi-factor authentication (MFA) to log in.

About MFA

Platform MFA has two components: [Creating Authentication Profiles](#) and [Creating Identity Policies](#).

- An authentication *profile* determines which MFA challenges are presented to a user (see [Creating Authentication Profiles](#)).
- An identity *policy* determines whether and when a user is presented with the challenges in their assigned MFA profile (see [Creating Identity Policies](#)).

For more information about MFA on the Delinea Platform, see the following sections:

- [Creating Identity Policies](#). Enabling MFA on the platform requires setting up identity policies and assigning them to users. An identity policy determines whether and when a user is presented with the challenges specified in the associated MFA profile.
- [Creating Authentication Profiles](#). Enabling MFA on the platform requires setting up authentication profiles. An authentication profile specifies the authentication challenges required to log in to the platform, and the length of time that must elapse before a user is re-prompted for authentication.
- [Using MFA Providers](#). Configuring MFA providers provides an additional layer of security to ensure proper authentication for users accessing the Delinea Platform.
- [Using MFA for Secrets](#). Multi-factor authentication (MFA) for secrets gives platform administrators the option to add one or more security requirements to access defined secrets.
- [Configuring IWA](#). The Delinea Platform can accept an Integrated Windows Authentication (IWA) connection as sufficient authentication for users with Active Directory accounts to log in to the platform.
- [Configuring Corporate IP Ranges](#). The Corporate IP Range function is used to define IP ranges for both internal and external networks and to define authentication requirements, such as the locations or IP ranges from which users can log in to the Delinea Platform.
- [Login Flow for the Delinea Platform Portal \(MFA\)](#). The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. Also see [Delinea Mobile Log in Process](#).
- [MFA Providers](#): Configuring MFA providers adds an additional layer of security to ensure that users accessing the Delinea Platform are properly authenticated:
 - [Configuring Duo Authentication](#)
 - [Configuring RADIUS Authentication](#)


Creating Authentication Profiles


To enable MFA on the platform, you must set up authentication profiles. An authentication profile specifies the authentication challenges required to log in to the platform and the length of time that must elapse before a user is prompted for authentication again.

Authentication profiles work with identity policies (see [Creating Identity Policies](#)), which determine whether and when a user is presented with the challenges specified in the associated authentication profile.

Authentication profiles also control step-up MFA flows on the platform, such as [Using MFA for Secrets](#).

Multi-Factor Authentication

 **Note:** Users can also log on to the platform using MFA on the Delinea Mobile application. For more information, see the following: [Delinea Mobile Overview](#), [Delinea Mobile Log in Process](#), [Logging In to the Delinea Platform \(MFA\)](#).

 **Note:** When creating a policy enabling a user to select or modify their authentication challenges (such as phone call, SMS, or FIDO2), do not require the user to complete the same challenge they are trying to set up. For example, when creating a policy enabling a user to select FIDO2 as an authentication challenge, do not use a **profile** that requires the user to complete the FIDO2 challenge. If you create such a defective policy, the user will be presented with the following error message: "Authentication Challenge Required. Cannot start step-up authentication flow. User does not have the attributes required to log in. Please contact your administrator."

View Authentication Profiles

Click **Settings** from the left navigation, then click **Authentication profiles**.

Authentication profiles

Create authentication profiles to manage how your Platform users are authenticated.
[Learn more about authentication profiles.](#)

[Add Authentication Profile](#)

Q Search...

4 items

To: Profile name

PROFILE NAME ↑	DESCRIPTION	CHALLENGES	CHALLENGE PASS-THRU
Default New Device Login Profile		2	12 hours
Default Other Login Profile		1	12 hours
Default Password Reset Profile		1	12 hours
Step Up Authentication Default	Default profile for Step Up Authentication	1	15 minutes

The platform comes with four built-in authentication profiles:

- **Default New Device Login Profile:** Uses Password for the first challenge. For the second challenge, gives the user options to use Mobile Authenticator, Text message (SMS) confirmation code, Email confirmation code, or OATH OTP Client. 12-hour pass-through duration.
- **Default Other Login Profile:** Uses Password for the first challenge. 12-hour pass-through duration.
- **Default Password Reset Profile:** Gives the user options to use Mobile Authenticator, Text message (SMS) confirmation code, Email confirmation code, or OATH OTP Client for the first challenge. 12-hour pass-through duration.
- **Step Up Authentication Default:** Gives the user options to use Email confirmation code or Mobile Authenticator. 15-minute pass-through duration.

You can review the details of each authentication profile by clicking directly on the profile name.

Add a New Authentication Profile

1. Click **Add Authentication Profile**.
2. Fill in the fields on the form:
 - **Profile name:** a unique name for the profile
 - **Description:** a brief description of the profile

Multi-Factor Authentication

- **Challenge pass-through duration:** Choose an option from the dropdown menu to set the time that must elapse before a user is prompted again for MFA authentication. Challenge pass-through duration only applies to step-up MFA requests and does not apply to platform log-ins. The default is 30 minutes.
- **Authentication challenges:** Select one or more of the authentication mechanisms available for Challenge 1 and Challenge 2.

Add Profile

Define an authentication profile by selecting from the available authentication challenges below. [Learn more about authentication profiles](#)

Profile name *

Description

Challenge pass-through duration

Authentication challenges

Choose from the available challenge options below.

Challenge 1*	Challenge 2
<input type="checkbox"/> Password / SSO	<input type="checkbox"/> Password / SSO
<input type="checkbox"/> Delinea Mobile Authenticator	<input type="checkbox"/> Delinea Mobile Authenticator
<input type="checkbox"/> Phone call	<input type="checkbox"/> Phone call
<input type="checkbox"/> Text message (SMS) confirmation code	<input type="checkbox"/> Text message (SMS) confirmation code
<input type="checkbox"/> Email confirmation code	<input type="checkbox"/> Email confirmation code
<input type="checkbox"/> OATH OTP client	<input type="checkbox"/> OATH OTP client
<input type="checkbox"/> 3rd Party RADIUS authentication	<input type="checkbox"/> 3rd Party RADIUS authentication
<input type="checkbox"/> FIDO2 authenticator	<input type="checkbox"/> FIDO2 authenticator
<input type="checkbox"/> Security questions	<input type="checkbox"/> Security questions

3. Click **Save**.



Note:

- Some authentication mechanisms, such as FIDO2, require additional configurations before users can authenticate with them.
- If a user is presented with multiple challenges, the platform waits until the user completes all challenges before giving the authentication response (pass or fail). For example, if the user enters the wrong password for the first challenge, the platform does not send the authentication failure message until after the user responds to the second challenge.
- If a user fails the first challenge, and the second challenge is SMS, email, or phone call, by default the platform will not send the SMS/email or trigger the phone call.
- Federated users can be prompted for additional MFA challenges within the platform. This applies to logging into the platform and any browser-based step-up MFA, such as step-up MFA for Secrets. The identity policy setting "Platform login via federation satisfies all MFA mechanisms" should be disabled to allow for this.
- Special consideration: As support for federated users for MFA has been recently enhanced, if you have enabled the platform integration with Secret Server to require multi-factor authentication, then access to the Secret Server application will be gated by MFA for all users, including federated

users. Ensure your federated users have appropriate MFA in place; otherwise, they cannot access the Secret Server application.

Authentication Challenges

You can select the authentication challenges available to users. However, the challenges actually presented to the user depend on the account's properties. For example, if you select all the mechanisms, but a user account has only a username and email address, the login prompt presents only those two challenges.

The following mechanisms are available:


- **Password/SSO:** The user is prompted for either their Active Directory password or Platform account password, or they are directed to the appropriate federation identity provider to complete the authentication.
- **Delinea Mobile Authenticator:** The user authenticates using a one-time passcode displayed in the Delinea mobile application on their mobile device. If the user's mobile device is connected through the cellular network or through a wi-fi connection, the user can send passcodes from the devices. If the user's mobile device is not connected in these ways, the user must manually enter the passcode in the login prompt.
- **Phone call:** Delinea Platform calls the user at the stored phone number (mobile or land line) and describes an action the user must complete to authenticate from the device to log in. Phone PIN must be enabled.
- **Text message (SMS) confirmation code:** The Delinea Platform sends a text message to the user's mobile phone with a one-time confirmation code, which the user must enter at the login prompt.
- **Email confirmation code:** The Delinea Platform sends an email to the user with a one-time confirmation code, which the user must enter at the login prompt.
- **OATH OTP client:** The user can use a third-party authenticator such as Google Authenticator to generate a one-time passcode (OTP). This authentication mechanism requires [additional configuration](#).
- **3rd Party RADIUS authentication:** The platform communicates with the client's RADIUS server to allow for user authentication to the platform.
- **FIDO2 authenticator:** FIDO2 is an authentication standard hosted by FIDO Alliance. FIDO2 includes the Web Authentication ("WebAuthn") API specification, written by the World Wide Web Consortium (W3C) and FIDO, with participation from third parties. The WebAuthn API is backward compatible with Universal 2nd Factor (U2F) keys. Delinea leverages the WebAuthn API to enable authentication to the platform without passwords, using either on-device authenticators or external authenticators. On-device authenticators are biometric authenticators integrated into the device hardware. Popular examples are Mac Touch ID, Windows Hello, and fingerprint scanners. External authenticators are security keys that you plug into the device's USB port, such as a YubiKey.
- **Security questions:** The user is prompted to answer security questions defined by the user or by a platform administrator. When creating an authentication profile, you can specify the number of questions the user must answer. You can also specify the number of user-defined and administrator-defined questions available to the user. A user can create or update any available user-defined question or answer from their platform user profile page.

Assigning a Login Authentication Profile

Once you have an appropriate authentication profile set up and enabled, the next step is to assign the profile to an identity policy. The following represents the bare minimum when setting up a policy:

Multi-Factor Authentication

1. Click **Access** from the left navigation, then click **Identity Policies**.
2. Click the name of a policy. (To add a new policy, see [Creating Identity Policies](#)).
3. Click the **Authentication** tab.
4. In the Services section, click **Edit**.
5. For **Enable authentication policy controls**, select the box next to **Enabled**.
6. Next to **Default authentication profile**, select an appropriate authentication profile from the drop-down menu. See **Important** warning below about the **Deny platform authentication** profile.
7. Optional: You can add **Authentication Rules** to define conditions for authentication challenge requirements. Each rule maps to a customizable authentication profile. If no rules are configured, the default profile is used.
8. Click **Save**.

 **Important:** If you select **Deny platform authentication** in the **Default authentication profile** drop-down and you configure no authentication rules, users will not be able to log in to the service. To use this profile appropriately, see "Create a Conditional Access Policy" on page 481



Notes:


- For optimal policy implementation, we recommend initially assigning the policy to only a small test user group before assigning it for real world use. This approach allows you to recover gracefully from issues that might arise, with minimal impact.

- Once you enable authentication policy controls, you can configure the rest of the policy options on the same page. For detailed information, see [Creating Identity Policies](#).

Global Security Settings

1. Click **Settings** from the left navigation, then select **Global Security**.
2. Click the **Configuration** tab. The page displays the global authentication options you can configure.

Global authentication options

Configure the global security settings that govern authentication profiles and MFA options. Global authentication settings are set to expert-recommended defaults that you can also customize. [Learn more about authentication configuration.](#) 

Edit

Authentication parameters	<input checked="" type="checkbox"/> Enable forgot username self-service at login		
	<input checked="" type="checkbox"/> Send email notification to users when password is changed		
Passcode length	6 characters		
Additional attributes for MFA	<table><thead><tr><th>ATTRIBUTE</th><th>TYPE</th></tr></thead></table>	ATTRIBUTE	TYPE
ATTRIBUTE	TYPE		

3. Click **Edit**. The page changes, enabling you to modify the settings used by MFA, such as phone numbers and email addresses. These settings include the following:

- **Authentication Parameters:**
 - a. **Enable forgot username self-service at login**

Allows a user to retrieve a forgotten username. The user is prompted to enter an email address, and if the email address matches a platform account, the platform sends the username to that email address.
 - b. **Send email notification to users when password is changed**

Sends an automated email after a user resets their platform password using the *forgot password* process.
- **Passcode Length:** You can set the confirmation passcode length to 6 or 8 digits. The default is 8 digits.
- **Additional Attributes for MFA:** You can add more attributes for MFA, such as other mobile phone, other home phone, other office phone, and other email addresses.

Security Questions

You can define questions that users can choose and answer to authenticate to the platform.

1. Click **Settings** from the left navigation, then select **Security Questions**.

Authentication

Authentication profiles

Configuration

Secret Server Connection

Security questions

Security devices

Create security questions to use in policies. [Learn more about security questions.](#)

Create Question

2 items

⌵ ⬇ ⌵

☐ SECURITY QUESTIONS ↑☐ What is your favorite movie?☐ What was the name of your first pet?

To add a security question:

1. Click **Create Question**.
2. Type a question in the text field.
3. Click **Add**.

Security Devices

Click **Settings** from the left navigation, then select **Security devices**.

Authentication

Authentication profiles

Configuration

Secret Server Connection

Security questions

Security devices

Mobile devices

OATH Tokens

FIDO2 Tokens

Review and manage FIDO2 authenticator registrations for users.

Q Search

5 items ⌵ User ▾

⌵ ⬇ ⌵

<input type="checkbox"/> USER ↑	TYPE	NAME	VALID	TOKEN ID	ENROLLED
<input type="checkbox"/> jsmith@example.com	SECURITYKEY	Yubikey	Valid	example.delinea.app	09/28/2023 01:06 pm
<input type="checkbox"/> ksmith@example.com	ONDEVICEAUTHENTICATOR	mac-fingerprint	Valid	example.delinea.app	12/20/2022 05:31 am

- The **Mobile devices** sub-tab displays instances of registered mobile applications with the associated users. The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. See [Logging In to the Delinea Platform \(MFA\)](#).
- The **OATH Tokens** sub-tab displays registered OATH tokens for third-party authenticators, such as Google Authenticator and Microsoft Authenticator.
- The **FIDO2 Tokens** sub-tab displays registered FIDO2 tokens for third-party authenticators, such as U2F, that use specialized Universal Serial Bus (USB) devices or near-field communication (NFC) devices.

Creating Identity Policies

To enable MFA on the Delinea Platform, you must set up identity policies and assign them to users. An identity policy determines whether and when a user is presented with the challenges specified in the associated Authentication profile (see [Creating Authentication Profiles](#)). Identity policies apply to all web log-ins to the Delinea Platform.



Note: Users can also log on to the platform using MFA on the Delinea Mobile application. For more information, see the following: [Delinea Mobile Overview](#), [Delinea Mobile Log in Process](#), [Logging In to the Delinea Platform \(MFA\)](#).



Note: When creating a policy enabling a user to select or modify their authentication challenges (such as phone call, SMS, or FIDO2), do not require the user to complete the same challenge they are trying to set up. For example, when creating a policy enabling a user to select FIDO2 as an authentication challenge, do not use a **profile** that requires the user to complete the FIDO2 challenge. If you create such a defective policy, the user will be presented with the following error message: "Authentication Challenge Required. Cannot start step-up authentication flow. User does not have the attributes required to log in. Please contact your administrator."

Create and Assign an Identity Policy

1. Click **Access** from the left navigation, then click **Identity Policies**.
2. Click **Add Policy**.
3. Optional: Select the box next to **State** if you wish to activate the policy.
4. Fill in the fields:
 - **Name:** (required) The name must be unique on the platform.
 - **Description:** (optional) The description should make it easy for others to identify the purpose of the policy.
5. At the top, select the **Enabled** checkbox if you wish to activate the policy.

Multi-Factor Authentication

Add policy

State ☐ Enabled

Name *

Description

Policy assignment *

Search or pick one

Global


Specific groups

affecting all users, groups, and service groups.
selected group(s).

- Next to **Policy assignment**, choose **Specific groups**. You can then apply the policy to specific users, groups, or service groups, tailoring the policy to the unique needs of different departments within your organization.

If you select **Global**, the policy will apply to all users, groups, and service groups across the entire tenant. For example, you could lock yourself and everyone else out of the platform, so choose this option with great care.

- Click **Next**.
- Search for a group or select one or more groups from the list.
- Click **Add** to create the policy.


 **Note:** For optimal policy implementation, consider assigning a new policy to a small test user group initially, before assigning it for real-world use. This approach allows you to recover gracefully from issues that might arise, with minimal impact.

Create a Conditional Access Policy

In some scenarios, a platform admin might need to allow platform log in access for specific groups while denying that access to other groups. For example, this functionality could improve the organization's security and compliance when integrating Active Directory into the platform.

On the Delinea Platform, a platform admin can set up this functionality using a combination of specific profile and policy settings.

If you select **Deny platform authentication** in the Default profile drop-down, and you configure no authentication rules in the next section, users will not be able to log in to the platform. This can be an efficient way to restrict users from gaining access to the platform.

 **Note:** To ensure that not ALL users are prevented from logging into the platform, make sure you assign some users appropriate log in policies and verify that those users can log in as expected.

Steps

Multi-Factor Authentication

- 1. Create a new policy with an intuitive name, such as *Disallow Login Policy*.
- 2. On the Authentication tab next to **Default authentication profile**, select **Deny platform authentication** from the drop-down.

OverviewPolicy assignmentAuthenticationUser securitySummary

Services

Applies to all web logins to the cloud service, including the platform and on-demand application authentication.
[Learn more about policies.](#)

Enable authentication policy controls

☐ Enabled

Default authentication profile

Deny platform authentication

Cancel

Save

Authentication Rules

Create rules to specify conditions for authentication challenge requirements. Each rule corresponds to a customizable authentication profile. If no rules are configured, the default authentication profile will be applied. Arrange rules in order of priority by moving the highest priority rule to the top. The rule at the top of the table will hold precedence in the policy, overriding the default authentication profile if applicable.

0 items

RULE NAME

AUTHENTICATION PROFILE

No items found

- 3. Configure no authentication rules.
- 4. Apply the policy to users you wish to prevent from logging into the platform.
- 5. Send the *Disallow Login Policy* you created to the bottom of the list to trigger last, because the platform searches policies for rules in stack ranked order. All policies *not at* the bottom should target the groups of users that need access to login to the platform.

Multi-Factor Authentication

Home

Secret Server

Inventory

Insights

Discovery

Policies

Access

Marketplace

Inbox

Settings

Access

Users

Groups

Roles

Identity policies

Administration > User Management >

Search the Delinea Platform

Identity Policies

Manage access policies for platform members. Policies can be arranged in order of priority with the highest priority at the top.

Search...

4 items

	NAME	STATUS	DESCRIPTION
1	Federated Users	Enabled	
2	AD Users	Enabled	Users in specific groups are allowed login to the platform.
3	Default Policy	Disabled	
4	Disallow Login Policy	Enabled	Policy to block unauthorized users outside of the allowed policies from logging in with their Active Direc...

The policy and policy order creates conditional access where only the Active Directory Group users are granted access...

Home

Secret Server

Inventory

Insights

Discovery

Access

Marketplace

Inbox

Settings

Access

Users

Groups

Roles

Identity policies

Identity policies >

Search

AD Users

Overview

Policy assignment

Authentication

User security

Summary

Configure policy assignment either globally (entire tenant) or for specific groups.

Edit

Policy assignment

Specific groups

Global: Apply policy to entire tenant, affecting all users, groups, and service groups. Specific groups: Apply policy only to selected group(s).

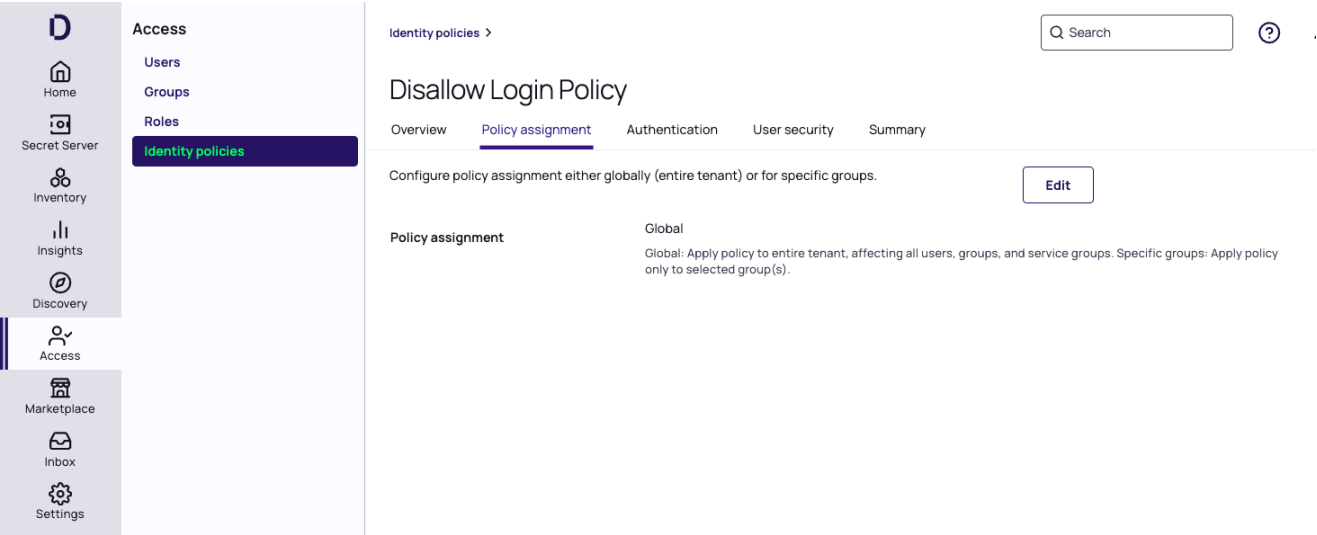
Search...

1 item

NAME ↑	DESCRIPTION
Internal Employees Demo Users	

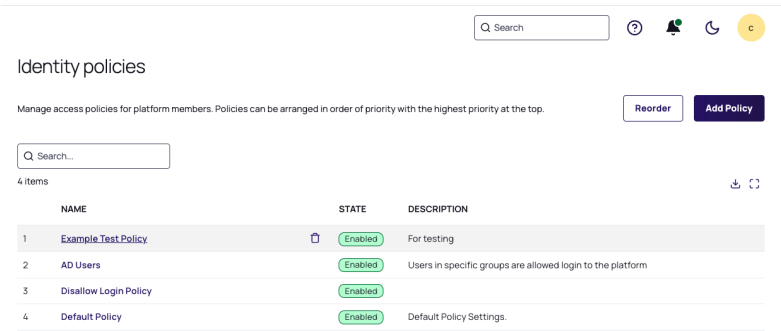
... and all other users, per the **Global** assignment, are not allowed to log in:

Multi-Factor Authentication



Update an Identity Policy

1. Click **Access** from the left panel, then click **Identity Policies**.
2. Click the policy you want to edit.



The policy page opens to the **Overview** tab, which displays the policy state, name, and description.

3. Click **Edit**.

Multi-Factor Authentication

Identity policies >

Q Search

Example Test Policy

Overview Policy assignment Authentication User security Summary

State **Enabled** Edit

Name Example Test Policy

Description For testing

4. If you want the policy to be active, select the box next to **Enabled** if it is not already selected.

Identity policies >

Q Search

Example Test Policy

Overview Policy assignment Authentication User security Summary

State ☒ Enabled

Name * Example Test Policy

Description For testing

Cancel Save

5. Update the **Name** and **Description** fields as desired.
6. To update the group policy assignment:
- Click the **Policy assignment** tab.
 - Click **Edit**.
 - Click **Assign Groups**.
 - Search for or select one or more groups from the list.
 - Click **Assign**.
 - To unassign a group from the policy, select the policy and click the trash icon next to the group name.
7. Click **Save**.

Authentication

Click the **Authentication** tab. The tab displays information on the policy's Services, Authentication Rules, Browser Session Parameters, Delinea Mobile Application Session Parameters, and Other Settings.

Services

1. In the Services section, click **Edit**.

Overview Policy assignment **Authentication** User security Summary

Services

Applies to all web logins to the cloud service, including the platform and on-demand application authentication. [Learn more about policies.](#)

Edit

Enable authentication policy controls Disabled

Default authentication profile None

2. For **Enable authentication policy controls**, select the box next to **Enabled**.

Services


Applies to all web logins to the cloud service, including the platform and on-demand application authentication. [Learn more about policies.](#)

Enable authentication policy controls ☒ Enabled

Default authentication profile Test Profile

Cancel **Save**

3. Select a default profile from the dropdown options.

 **Note:** If you select **Deny platform authentication** from the **Default authentication profile** drop-down, and you configure no authentication rules in the next section, users will not be able to log in to the service.

4. Click **Save**.

Once you enable authentication policy controls, you can configure the rest of the policy options on the same page.

Authentication Rules

Build rules to define conditions for authentication challenge requirements. Each rule maps to a customizable authentication profile. The default profile is used if no rules are configured.

1. In the Authentication Rules section, click **Edit**.

Authentication Rules **Edit**

Move up or move down rule to specify order. The highest priority is on top. If applicable, the rule displayed at the top of the table will be applied to the policy and will override the default profile.

1 item ⬇ ⌂

	RULE NAME	AUTHENTICATION PROFILE
1	Identity cookie is not present	Default New Device Login Pr...

2. Click **Add rule**.

Multi-Factor Authentication

Add an Authentication rule

Name *

Enter rule name

Authentication profile *

Select a profile

- 3. Enter a **Name** for your new authentication rule.
- 4. Select an **Authentication profile** to associate with the rule.
- 5. Click **Add new filter**.
- 6. Select the desired Filter.

Add new filter

Name *

IP range

Authentication profile *

Test Profile

Authentication Filters

+ Add new filter

Filter

IP address

Condition

Search or pick one

inside corporate IP range

outside corporate IP range

Cancel

Add

- 7. Select the desired Condition.
- 8. Click **Save**.
- 9. Add more filters as desired.
- 10. After adding filters, click **Add**. Your new rule appears on the Authentication Rules page, with its name and authentication profile displayed.

Available Settings	Description
Authentication Rules	Build rules to define conditions for authentication challenge requirements. Each rule maps to a customizable authentication profile. The default profile is used if no rules are configured.
Default Profile	The profile platform used if no profile is added/selected. New profiles can be added from here or from Settings > Authentication Profiles .

Browser Session Parameters

1. In the **Browser Session Parameters** section, click **Edit**.
2. Use the following table to make your selections, then click **Save**.

Available Settings	Description
Allow 'Keep me logged in' checkbox option at login (session spans browser sessions)	Enables the user to select the option to select Keep me logged in at login. Persists session cookies across browser sessions.
Session Length (in Hours)when 'Keep me logged in' option enabled	Number of hours "Keep me logged in" checkbox enabled by default for users. Default = 12 hours, minimum value = 1 hour, maximum value = 24 hours
User Idle Timeout	The value is set in minutes. It controls the idle time before the user's session expires. Default = 15 minutes, minimum value = 1 minute, maximum value = 720 minutes.



Note: The platform's User Idle Timeout for browser sessions applies equally to PRA sessions. You cannot modify user idle timeout settings specifically for PRA connections.

Delinea Mobile Application Session Parameters

1. In the **Delinea Mobile Application Session Parameters** section, click **Edit**.
2. Use the following table to make your selections, then click **Save**.

Available Settings	Description
Session Length (Days)	Applicable to the Delinea Mobile App only. This setting keeps the user's session alive on the mobile app. When the session length is reached, the user must authenticate with the platform again. Default = 14 days, minimum value = 1 day, maximum value = 90 days.

Other Settings

In the **Other Settings** section, click **Edit**.

Other Settings

IWA connections

- ☐ Allow IWA connections (bypasses authentication rules and default profile)
- ☐ Set identity cookie for IWA connections
- ☐ IWA connections satisfy all MFA mechanisms

Other

- ☒ Allow users without a valid authentication factor to log in
- ☐ Disable interactive service user login
- ☒ Platform login via federation satisfies all MFA mechanisms
- ☒ Allow additional authentication from same device
- ☐ Continue with additional challenges after failed challenge
 - ☐ Do not send challenge request when previous challenge response failed
- ☐ Remember and suggest last used authentication factor

Use the following information to make your selections, then click **Save**.

IWA Connections

- **Allow IWA Connections (bypasses authentication rules and default profile)**

Allows platform to bypass already configured authentication rules and default authentication profiles when IWA is configured. This option is configured by default.

- **Set identity cookie for IWA Connections**

Enables the platform to write a cookie in the current browser after a successful IWA-based log in. The platform checks the browser for this cookie when the user logs in to the platform. As long as the cookie is there, the user is not prompted for multi-factor authentication.

- **IWA Connections satisfy all MFA mechanisms**

Optional. Configure Delinea Platform to use IWA to override all application-specific authentication requirements.

Other

- **Allow users without a valid authentication factor to log in**

Exempts users from multi-factor authentication when their account does not contain a mobile phone number and email address, and cannot satisfy the applied policies.

- **Disable interactive service user login**

Disabled by default. Enabling this option disables interactive login for service users.

Multi-Factor Authentication

- **Platform log in via federation satisfies all MFA mechanisms**

Enabled by default. If a user is successfully authenticated through Federation, they will not be required to complete additional MFA steps.

- **Allow additional authentication from same device**

Disable this option to block all authentication methods to the same device except Password, Email, Security Questions, and 3rd Party RADIUS.

- **Continue with additional challenges after failed challenge**

Notifies users of a failed authentication after the first failed challenge.

- **Do not send challenge request when previous challenge response failed**

Configures the platform to handle the default MFA behavior (allow users to step through all the relevant MFA challenges before we notify them of their failed authentication attempt) differently, based on the challenge type.

- **Remember and suggest last used authentication factor**

Remember the authentication method that was used most recently.

User Security

Click the **User Security** tab, where you can configure settings under sub-tabs for Self Service, Password Settings, OATH OTP, RADIUS, User Account Settings, and Authentication Settings.

Self Service

1. Click the **Self Service** sub-tab.
2. Click **Edit**, then select **Enabled**.
3. Click **Save**.

The page displays three configuration areas:

- Password Reset
- Account Unlock
- Additional Policy Parameters

Password Reset

1. Click **Edit**.
2. **Password reset status**: select **Enabled**.
3. Select one or more of the checkboxes:
 - **Allow for Active Directory Users**
 - **Only allow from browsers with identity cookie**
 - **User must log in after successful password reset**
4. **Password reset authentication profile**: Select **Default Password Reset Profile** from the drop-down. When a user clicks "forgot password" at the platform log in page, the **Default Password Reset Profile** presents the user

Multi-Factor Authentication

with one or two non-password challenges. When the user meets these challenges, the user is presented with the reset password workflow.

5. **Maximum consecutive password reset attempts per session:** Select the desired number of reset attempts from the dropdown list.

Account Unlock




Note: Account Unlock applies to local/AD accounts only. It does not apply to federated accounts.

1. **Account unlock status:** select **Unlocked**.

Account Unlock

Choose account unlock options to match your security needs.

Account unlock status	<input checked="" type="checkbox"/> Unlocked
Account unlock parameters	<input type="checkbox"/> Allow account unlock for Active Directory users <input type="checkbox"/> Only allow account unlock from browsers with identity cookie <input type="checkbox"/> Show a message to end users that account is locked in desktop login (default no)
Account unlock authentication profile *	Default New Device Login Profile
Active Directory self service settings	<input checked="" type="radio"/> Use a connector running on a privileged account <input type="radio"/> Use these credentials
Administrator user name	Enter username
Administrator password	Enter password 

2. **Account Unlock Parameters:** Select one or more checkboxes:
 - Allow account unlock for Active Directory Users
 - Only use account unlock from browsers with identity cookie
 - Show a message to end users in desktop login that account is locked (default: no)
3. **Account unlock authentication profile:** Select a profile from the dropdown list.
4. If you checked **Allow account unlock for Active Directory Users**, you can choose a setting in **Active Directory self service settings**:
 - Use connector running on privileged account
 - Use these credentials
5. If you select **Use these credentials**, fill in the fields for **Admin User Name** and **Admin User Password**.

Multi-Factor Authentication

The screenshot shows the 'Account Unlock' configuration page. At the top, it says 'Choose account unlock options to match your security needs.' Below this, there are several sections: 'Account Unlock Parameters' with a checked 'Enable' checkbox and three sub-options (all checked: 'Allow account unlock for Active Directory users', 'Only allow account unlock from browsers with identity cookie', and 'Show a message to end users in desktop login that account is locked (default no)'); 'Account Unlock Authentication Profile *' with a dropdown menu set to 'Default New Device Login Profile'; 'Active Directory Self Service Settings' with two radio buttons, the second of which ('Use these credentials') is selected; 'Admin User Name *' with a text input field containing a redacted name; and 'Admin User Password *' with a password input field containing redacted characters and an eye icon. At the bottom right are 'Cancel' and 'Save' buttons.

6. Click **Save**.

Additional Policy Parameters

1. Click **Edit**.
2. Select the desired options from the dropdown menus:
 - **Maximum forgotten password resets allowed within window (default: 10)**
 - **Capture window for forgotten password resets (default: 60 minutes)**

The screenshot shows the 'Additional Policy Parameters' configuration page. It starts with the title 'Additional Policy Parameters' and the subtitle 'Change additional policy parameters here.' Below this is a section titled 'Parameters'. It contains two dropdown menus: 'Maximum forgotten password resets allowed within window (default 10)' set to '3 resets', and 'Capture window for forgotten password resets (default 60 minutes)' set to '20 minutes'. At the bottom right are 'Cancel' and 'Save' buttons.

3. Click **Save**.

Password Settings

1. Click the **Password Settings** sub-tab. The following fields are displayed:
 - Password Requirements
 - Display Requirements
 - Additional Requirements
 - Password Age
 - Capture Settings

Password Requirements

1. Click **Edit**.

Password Requirements

You can select the password reset options to enforce password security for users.

Password Length

Minimum password length (default 8)

5 characters

Maximum password length (default 64)

8 characters

Password Complexity Requirements

Require at least one digit (default yes)

Enabled

Require at least one upper case and one lower case letter (default yes)

Enabled

Require at least one symbol (default no)

Not Set

2. Make your selections for **Password Length** and **Password Complexity Requirements**.
3. Click **Save**.

Display Requirements

1. Click **Edit**.

Display Requirements

Password Complexity Requirements

Show password complexity requirements when entering a new password (default no)

Enabled

Password complexity requirements for directory services other than Delinea Directory

Cancel

Save

2. Make your choices for the following:
 - **Show password complexity requirements when entering a new password (default: no)**
 - **Password complexity requirements for directory services other than Delinea Directory**
3. Click **Save**.

Multi-Factor Authentication

Additional Settings

1. Click **Edit**.

Additional Requirements

Check against weak password	Enabled ▾
Allow username as part of password	Disabled ▾
Allow display name as part of password	Disabled ▾
Require at least one Unicode characters	Disabled ▾
Limit the number of consecutive repeated characters	5 characters ▾

2. Make your selections from the drop-down lists:
 - Check against weak password
 - Allow username as part of password
 - Allow display name as part of password
 - Require at least one Unicode character
 - Limit the number of consecutive repeated characters
3. Click **Save**.

Password Age

1. Click **Edit**.

Password Age

Password Age Parameters

Minimum password age before change is allowed (default 0 days)	1
Maximum password age (default 365 days)	365
Password history (default 3)	3 passwords ▾

Password Expiration Notification

Password Expiration Notification (default 14 days)	21 days ▾
Escalated Password Expiration Notification (default 48 hours)	48 hours ▾
Enable password expiration notifications on enrolled mobile devices	Enabled ▾

2. Make your selections for **Password Age Parameters** and **Password Expiration Notification**.
3. Click **Save**.

Capture Settings

1. Click **Edit**.

Capture Settings

Maximum consecutive bad password attempts allowed within window (default Off)

Off

Capture window for consecutive bad password attempts (default 30 minutes)

30

Lockout duration before password re-attempt allowed (default 30 minutes)

30

2. Make your selections from the dropdown lists:
- Maximum consecutive bad password attempts allowed within window (default: off)
 - Capture window for consecutive bad password attempts (default: 30 minutes)
 - Lockout duration before password re-attempt allowed (default: 30 minutes)
3. Click **Save**.

OATH OTP

1. Click the **OATH OTP** sub-tab.
2. Click **Edit**.

Self Service

Password Settings

OATH OTP

User Account Settings

You can use a one-time-passcode (OTP) to login to this platform.
Any authenticator app that supports the OATH TOTP standard is supported.

OATH OTP Integration

Enable OATH OTP Integration

Enabled

3. Select **Enabled** from the dropdown list.
4. Click **Save**.

RADIUS

1. Click the **RADIUS** sub-tab.
2. Select **Enabled** from the dropdown list to enable RADIUS.

3rd Party RADIUS authentication

Enable 3rd Party RADIUS authentication

Not Set

Enabled

Disabled

Not Set

User Account Settings

- 1. Click the **User Account Settings** sub-tab.
- 2. Click **Edit**.

User SecuritySummary

User Account SettingsAuthentication Settingsation Settings

You can enable users to perform certain tasks related to their accounts.

Authentication Profile required to modify Personal ProfileDefault New Device Login Profile

- 3. Make your selection from the dropdown list.
- 4. Click **Save**.

Authentication Settings

- 1. Click the **Authentication Settings** sub-tab. Each authentication setting is labeled either **Active** or **Not Set**.
- 2. Click **Edit**.

Multi-Factor Authentication

Configuration

Authentication

User security

Summary

Self service

Password settings

OATH OTP

RADIUS

User account settings

Authentication settings

You can enable users to perform certain tasks related to their accounts.

Edit

Enable users to change their passwords

This policy determines whether users can change their passwords from the Account page, independent of the policies available under Password reset. The "Not Set" status here is equivalent to "Enabled".

Not Set

Enable users to enroll FIDO2 authenticators

This policy determines whether users can enroll FIDO2 authenticators to authenticate to the platform. Enable this option to display the security key and on-device authenticator options for users. The "Not Set" status here is equivalent to "Disabled".

Not Set

Enable users to configure an OATH OTP client (requires enabling OATH OTP policy)

This policy is typically used when you bulk upload OATH tokens (for example, those generated by a YubiKey). Enable this option to display the QR code to users. Disable it to hide the QR code from users. The "Not Set" status here is equivalent to "Enabled".

Not Set

Enable users to configure Security questions

Require users to set up and authenticate using security questions. When this policy is enabled, users must configure one security question.

Not Set

Enable users to configure a phone PIN for MFA

A phone PIN is required for users to authenticate via phone call.

Not Set

Require users to register device at sign in to use Mobile Authenticator

Not Set

The page displays the following sections. Under each section heading is a dropdown list where you can choose Enabled, Disabled, or Not Set:

- Enable users to change their passwords
- Enable users to enroll FIDO2 authenticators
- Enable users to configure OATH OTP client (requires enabling OATH OTP policy)
- Enable users to configure Security questions
- Enable users to configure a Phone PIN for MFA
- Require users to register device at sign in to use Mobile Authenticator.



Note: The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. See [Logging In to the Delinea Platform \(MFA\)](#).

3. Make your desired choices in each section.

Multi-Factor Authentication

For each user capability that you enable, more fields appear where you can configure additional settings, including the authentication profile required for the user to access the capability, as shown in the images below.



Note: When selecting a profile in *Authentication profile required to...*, do not select the default user login profile. If you do, the user could get locked out of the platform by entering an endless authentication loop.

Enable users to change their passwords

Enable users to change their passwords

This policy determines whether users can change their passwords from the Account page, and is independent of the policies available under Password Reset. The "undefined" status here is equivalent to "enabled."

Enabled

Authentication Profile required to change password

Enable users to enroll FIDO2 Authenticators

Enable users to enroll FIDO2 Authenticators

This policy determines whether users can enroll FIDO2 authenticators to authenticate to Delinea. Enable to display the Security Key and On-Device Authenticator options for users. The "undefined" status here is equivalent to "disabled."

Enabled

Require users to configure FIDO2 Security Key at sign in

Enabled

Require users to configure On-device authenticator Key at sign in

Enabled

FIDO2 Security Key Display Name *

Authentication Profile required to configure FIDO2 Authenticators

Enable users to configure an OATH OTP client

Enable users to configure an OATH OTP client (requires enabling OATH OTP policy)

This policy is typically used when you bulk upload OATH tokens (for example, those generated by a YubiKey). Enable this option to display the QR code to users. Disable it to hide the QR code from users. The "undefined" status here is equivalent to "enabled."

Enabled

Require users to configure at sign in

Enabled

OATH OTP Display Name *

OAUTH

Authentication Profile required to configure OATH OTP client

Enable users to configure Security Questions

Enable users to configure Security Questions

This policy determines whether configuring security questions is required for users to authenticate using security questions. When enabled, by default users are required to configure one security question.

Enabled

Require users to configure at sign in

Enabled

☒ Allow duplicate security question answers

Required number of user-defined questions *

1

Required number of admin-defined questions *

1

Minimum number of characters required in answers *

5

Authentication Profile required to set Security Questions

Multi-Factor Authentication

Enable users to configure a Phone PIN for MFA

Enable users to configure a Phone PIN for MFA

A phone PIN is required for users to authenticate via phone call.

Enabled

Require users to configure at sign in

Enabled

Minimum Phone PIN length

4 characters

Authentication Profile required to configure a Phone PIN

Cancel

Save

Require users to register device at sign in to use Mobile Authenticator

Require users to register device at sign in to use Mobile Authenticator

Enabled

Enabled

Disabled

Not Set


Cancel

Save


4. When you are finished making your selections, click **Save**.

The page displays the sections listed below, and under each section heading is a dropdown menu where you can choose Enabled, Disabled, or Not Set:

- Enable users to change their passwords
- Enable users to enroll FIDO2 Authenticators
- Enable users to configure OATH OTP client (requires enabling OATH OTP policy)
- Enable users to configure Security Questions
- Enable users to configure a Phone PIN for MFA
- Require users to register device at sign-in to use Mobile Authenticator.

 **Note:** The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. See [Logging In to the Delinea Platform \(MFA\)](#).

For each user capability that you enable, more fields appear where you can configure additional settings, including the authentication profile required for the user to access the capability, as shown in the images below.

 **Note:** When selecting an *Authentication profile required to...*, do not select the default user login profile. If you do, the user could get locked out of the platform by entering an endless authentication loop.

Enable users to change their passwords

Enable users to change their passwords

This policy determines whether users can change their passwords from the Account page, and is independent of the policies available under Password Reset. The "undefined" status here is equivalent to "enabled."

Enabled

Authentication Profile required to change password

Enable users to enroll FIDO2 Authenticators

Delinea Delinea Platform

Administrator Guide

Page 499 of 846

Multi-Factor Authentication

Enable users to enroll FIDO2 Authenticators

This policy determines whether users can enroll FIDO2 authenticators to authenticate to Delinea. Enable to display the Security Key and On-Device Authenticator options for users. The "undefined" status here is equivalent to "disabled."

Enabled

Require users to configure FIDO2 Security Key at sign in

Enabled

Require users to configure On-device authenticator Key at sign in

Enabled

FIDO2 Security Key Display Name *

Authentication Profile required to configure FIDO2 Authenticators

Enable users to configure an OATH OTP client

Enable users to configure an OATH OTP client (requires enabling OATH OTP policy)

This policy is typically used when you bulk upload OATH tokens (for example, those generated by a YubiKey). Enable this option to display the QR code to users. Disable it to hide the QR code from users. The "undefined" status here is equivalent to "enabled."

Enabled

Require users to configure at sign in

Enabled

OATH OTP Display Name *

OAUTH

Authentication Profile required to configure OATH OTP client

Enable users to configure Security Questions

Enable users to configure Security Questions

This policy determines whether configuring security questions is required for users to authenticate using security questions. When enabled, by default users are required to configure one security question.

Enabled

Require users to configure at sign in

Enabled

☒ Allow duplicate security question answers

Required number of user-defined questions *

1

Required number of admin-defined questions *

1

Minimum number of characters required in answers *

5

Authentication Profile required to set Security Questions

Enable users to configure a Phone PIN for MFA

Enable users to configure a Phone PIN for MFA

A phone PIN is required for users to authenticate via phone call.

Enabled

Require users to configure at sign in

Enabled

Minimum Phone PIN length

4 characters

Authentication Profile required to configure a Phone PIN

Cancel

Save

Require users to register device at sign-in to use Mobile Authenticator

Require users to register device at sign in to use Mobile Authenticator

Enabled

Enabled

Disabled

Not Set

Cancel

Save

Delinea Delinea Platform

Administrator Guide

Page 500 of 846

When you are finished making your selections, click **Save** at the bottom of the page.



Note: Users with the *Manage Identity Settings* permission can bypass the required MFA setup. See "Platform Permissions" on page 212

Summary

The **Summary** tab displays comprehensive information about the configured identity policy settings. The page does not provide editing capabilities, because all of these policies are added, changed, and removed elsewhere.

Using a FIDO2 Security Key

MFA always requires setting up an authentication profile and setting up an identity policy linked to that authentication profile. To use a hardware security key such as FIDO2, you must set it up in your user profile, your authentication profile, and your identity policy.

In your [User Profile](#), set up your personal FIDO key.

Click your user icon > **Account details** > **Security** tab > **Fido2** > configure > **Save**.

In the [Authentication profile](#) you're going to use, add **FIDO2 authenticator** as an authentication challenge.

Click **Settings** > **Authentication profiles** > select the profile > **Edit** > select **FIDO2 authenticator** > **Save**.

In the [Identity policy](#) linked to the authentication profile you're going to use, select **Enable users to enroll FIDO2 authenticators**.

Click **Access** > **Identity policies** > select the policy > **User security** tab > **Authentication settings** sub-tab > **Edit** > **Enable users to enroll FIDO2 authenticators** > **Save**.

Using MFA for Secrets

Multi-factor authentication (MFA) for secrets gives Delinea Platform administrators the option to add one or more security requirements to access specified secrets. This functionality is available exclusively through the Delinea Platform and supports many types of MFA, such as email, the Delinea Mobile App, YubiKey, and other devices using the FIDO2 protocol.

Availability

MFA for Secrets is available to all customers automatically. No initial global configuration is required to enable the feature. Secrets have the feature disabled by default, but you can easily enable it on an individual secret or on multiple secrets simultaneously. For example, if you apply a secret policy to a folder that enables MFA on secrets, all secrets added to that folder inherit the policy setting enabling MFA.

Default MFA Profile

When MFA is enabled on a secret, the **Step-up Authentication Default** profile applies to the secret. This profile uses email for the default authentication mechanism, and because the email is already in the user database, the user does not need to configure anything. Although the email mechanism is easiest for the user, there may be situations that call for a login mechanism stronger than email.

For information on viewing, managing and assigning authentication profiles, and on selecting challenges for the profiles, see [Creating Authentication Profiles](#).



Note: If you wish to modify a secret that requires MFA, you will be prompted with an MFA challenge before you can make any changes.

Assigning MFA to Secrets

You can assign MFA to secrets several ways:

- Assign MFA to an individual secret
- Assign MFA to a secret policy
- Assign MFA to a secret through a bulk operation

Assign MFA to an Individual Secret

1. Click **Secret Server** from the left navigation.
2. On the All Secrets page, click the name of a secret in the table. The page for that secret appears.



Note: The enabled secret in this case inherits a default authentication profile selected on a global level.

3. Select the **Security** tab.
4. In the **Multi-factor Authentication** section, click **Edit**.
5. Select the box next to **Require Multi-factor Authentication**.
6. Click **Save**.

Assign MFA to a Secret Policy

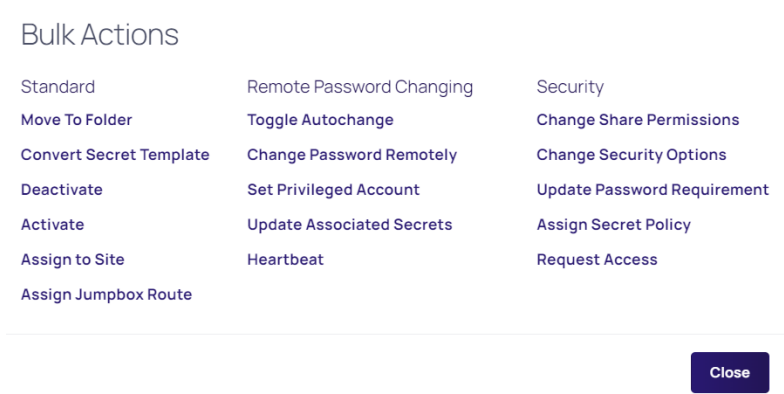
1. Click **Settings** from the left navigation, then click **Administration**.
2. Under Core Actions, click **Secret Policies**.
3. Click a policy.
4. Select the **Security** tab.
5. Click **Edit**.
6. Next to **Require Multi-factor Authentication**, select **Yes** from the dropdown list.
7. Click **Save**.

Assign MFA to Secrets Through a Bulk Operation

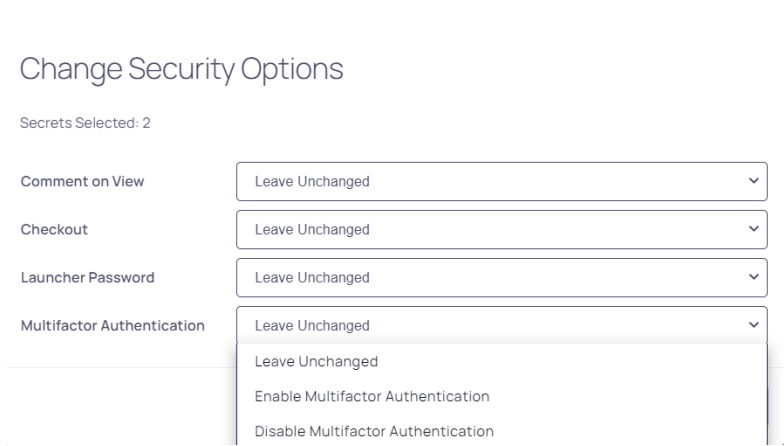
1. Click **Secret Server** from the left navigation.
2. On the All Secrets page, select the checkboxes for two or more secrets.
3. In the small banner that appears, click **Bulk Actions**.

Multi-Factor Authentication

4. In the **Bulk Actions** dialog, under **Security**, click **Change Security Options**.



5. Next to **Multi-factor Authentication**, select **Enable Multi-factor Authentication** from the dropdown list.

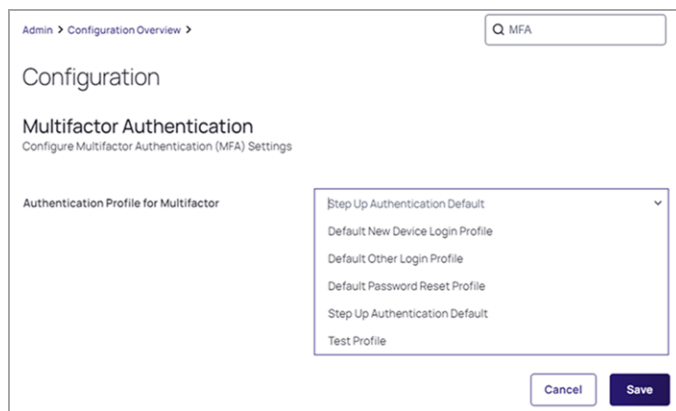


6. Click **Save**.

Applying an MFA Profile to All Enabled Secrets

1. Click **Settings** from the left navigation, then click **Administration** under Secret Server.
2. On the Secrets Administration page, click **Security MFA authentication** under Security.

Multi-Factor Authentication



The screenshot shows a web interface for configuring Multifactor Authentication (MFA). At the top, there is a breadcrumb trail: "Admin > Configuration Overview >". To the right of the breadcrumb is a search bar containing "Q MFA". Below the breadcrumb, the page title is "Configuration". Underneath, it says "Multifactor Authentication" and "Configure Multifactor Authentication (MFA) Settings". The main section is titled "Authentication Profile for Multifactor". It contains a dropdown menu with the following options: "Step Up Authentication Default" (which is selected), "Default New Device Login Profile", "Default Other Login Profile", "Default Password Reset Profile", "Step Up Authentication Default", and "Test Profile". At the bottom right of the form are two buttons: "Cancel" and "Save".

3. Click **Edit**.
4. Select an MFA profile from the dropdown list.
5. Click **Save**.

Considerations for Assigning MFA to Secrets

Note the following when configuring or assigning MFA to secrets:

- Secrets with MFA enabled are accessible in a disaster recovery replica by an administrator with unlimited permissions. The MFA requirement remains intact.
- When exporting secrets, if any secret in the selected list has MFA enabled, you are prompted for MFA.
- The profile you selected for secret MFA does not affect the profile for authenticating to the Delinea Platform.
- Secret Server Cloud cannot access MFA-protected secrets unless it was itself authenticated through the platform. If this authentication was not done, the user is prompted with a link to redirect to the secret in the platform.
- MFA-enabled secrets are not available in the Secret Server mobile application.

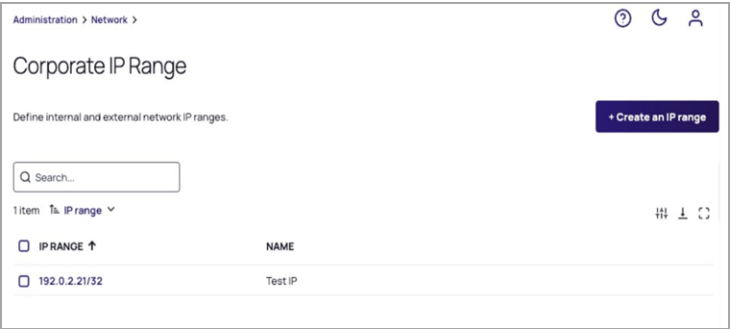
Configuring Corporate IP Ranges

The Corporate IP Range function is used to define IP ranges for both internal and external networks, and to define authentication requirements such as the locations or IP ranges from which users can log in to the Delinea Platform. For more information on using IP ranges in identity policies to control authentication when inside or outside a corporate IP range see [Authentication Rules](#).

To manage corporate IP ranges, use the following procedures.

1. Click **Settings** from the left navigation, then select **Corporate IP Range**.

Multi-Factor Authentication



Add an IP Range

1. Click **Create IP Range**.
2. In the **Create IP Range** dialog, fill out the fields for **IP Range or Address** and **IP Range Name**.

A screenshot of the 'Create an IP range' dialog box. The title is 'Create an IP range'. Below the title is a subtitle 'Enter an IP range or address and IP range name. Click Add to save the IP range.' There are two input fields: 'IP range or address *' with the value '192.0.2.22/32' and 'IP range name' with the value 'Test Range'. Below the first field is an example: 'Example: 65.12.116.12/2 or 65.12.116.42.' At the bottom right are 'Cancel' and 'Add' buttons.

3. Click **Add**.

Edit an IP Range

1. Click the IP range you wish to edit.
2. Update the settings as necessary.
3. Click **Save**.

Delete an IP Range

1. Select or hover on the IP range you wish to delete, and press the Delete key.
2. When prompted to confirm, click **Delete**.

Configuring IWA

The Delinea Platform enables you to accept Integrated Windows Authentication (IWA) as sufficient authentication for Active Directory user accounts to log in to the platform. The platform uses Kerberos SSO for authentication. With IWA enabled, the browser uses the current user's Active Directory information to prove its knowledge of the password through a cryptographic exchange with the in-process web server built into the Delinea Connector.

Multi-Factor Authentication

If you have multiple connectors enabled for IWA, the platform connects with the connectors according to the following priorities:

1. Any connector using the same IP address as the user's client machine.
2. If multiple connectors are using the same IP address as the user's client machine, the platform chooses one of them randomly. Multiple machines inside your network may appear as the same IP externally.
3. If a connector does not use the same IP address as the user's client machine, the platform chooses the best subnet match.
4. If none of the previous scenarios apply, the platform chooses a connector randomly.

Prerequisites

Before you start configuring IWA on the platform, make sure you have done the following:

- Your company has at least one Delinea Connector with the web server enabled.
- That connector must be joined to Active Directory in the forest to which users are authenticating.

Enabling IWA Service on the Delinea Connector

IWA is disabled by default when you install the Delinea Connector. To enable the connector, you must provide a certificate to the connector that will be present on endpoints.

To configure IWA and import the certificate:

1. Click **Settings** from the left navigation, then click **Connectors**.
2. Select the relevant connector or add a new one.
3. Select the IWA service tab, then click **Edit**.

You can modify the following settings:

Setting	Description
Enable web server	The default value is Enabled. This setting supports IWA and Office clients. If you disable the web server, you cannot change the DNS Hostname, HTTP Port Number and HTTPS Port number values.
DNS Hostname	The default is the name of the connector's host computer. You can enter a DNS short name here or the fully qualified domain name in the IE local intranet zone.
IWA Detection Timeout	The length of time IWA will wait for response from the connector. Default: 10 seconds.

Setting	Description
HTTPS Port Number	The default port is 8443. Port 8443 is the standard port. If you change the port number to a non-standard number, Firefox and Chrome may require additional configuration, because these browsers block some non-standard ports. Do not change the port number unless you know about the implications.
Connector Host Certificate	To activate IWA, you must provide a .pfx or .p12 certificate that is either trusted or self-signed. We strongly advise that the certificate be trusted by a Certificate Authority (CA). After you upload the certificate, if needed, you can conveniently download the public key certificate.

- Click **Save**.
- Click **Settings > Corporate IP Range**.
- Click **Create IP Range** to enter your corporate IP range. IWA will not work for users whose computers are outside of the defined corporate IP range.
- Click **Add**.
- Reboot your Delinea Connector if you have uploaded a certificate.

Obtaining a Delinea Connector IWA Host Certificate

To activate IWA, you must provide a trusted certificate issued by a Certificate Authority, or a self-signed .pfx or .p12 certificate. After you upload the certificate, you can download the public key certificate when needed. You can obtain an IWA Connector Host Certificate using any of the following processes:

- Request the Delinea Platform to generate a certificate for you. See ["Using an Automatically Generated Delinea Connector IWA Host Certificate"](#) below.
- Obtain a certificate from a trusted external certificate authority (CA) such as Symantec or GoDaddy. See ["Importing a Certificate"](#) on the next page.
- Generate your own certificate using an internal CA. This would not require trusting it on each endpoint, presuming you have other mechanisms in place to ensure that those endpoints trust their CA. As such, this may be as good as, or better than (depending on the company infrastructure) a trusted external CA.
- Generate a self-signed certificate, which would require trusting it on each endpoint it is used on (or through other policy/management infrastructure). See ["Generating a Self-Signed Delinea Connector IWA Host Certificate"](#) on page 509.

Using an Automatically Generated Delinea Connector IWA Host Certificate

- Click **Settings** from the left navigation, then click **Connectors**.
- Click the name of the machine where Delinea Connector is installed.
- Select the **IWA service** tab, then click **Edit**.

Multi-Factor Authentication

4. In **DNS hostname**, enter the FQDN of the Connector machine.
5. In **IWA detection timeout**, accept the default value or provide your desired value.
6. In the **HTTPS port number** field, enter **8443**. For MFA on PCS, endpoints that need to do MFA must be able to contact the Connector on 8443 and 8080.
7. Next to *Connector host certificate*, click **Generate certificate**.
8. Click **+Generate certificate**.

Wait for the platform to generate the certificate. A message like "Certificate successfully generated" appears, with the certificate details such as thumbprint, valid dates, and more.
9. In Web Server, click **Enabled**.
10. Click **Save**.

Importing a Certificate

If you are using internal or third-party CAs, you need to import those certificates to the platform. You can import wild card certificates.

To import a certificate to the platform:

1. From the left navigation menu, click **Settings**, then click **Connectors**.
2. Click the name of the machine where Delinea Connector is installed.
3. Select the **IWA Service** tab.
4. Click **Edit**.
5. Confirm that the **Enabled** box next to **Web Server** is selected.
6. In Connector host certificate, click **Upload certificate** to import an internal or third-party certificate. You can upload the same certificate to all Delinea Connectors in the same domain. If you do this, make sure you upload the same certificate to all IWA configured connectors. Ensure the subject of the certificate explicitly matches the hostname of the connector, or matches by using a wildcard in the subject.
7. Click **Select file**.
8. Browse to and select the host certificate file (.pfx or .p12 formats are supported).
9. Click **Open**.
10. Enter the password you used when running the PowerShell script to generate the certificate.
11. Click **Save**.
12. You must restart the Delinea Connector after importing the certificate.

Certificate Metadata:

- **Thumbprint:** A unique cryptographic hash value that identifies the certificate's content.
- **Not valid before and after:** The validity period specifies when the certificate becomes active ("Not valid before") and when it expires ("Not valid after").

- **Issuer:** The entity that issues the digital certificate, providing assurance about the accuracy of the subject's information.
- **Subject:** Identifies the entity to which the certificate is issued, including details such as common name, organization, and location.
- **Public key certificate:** Upon uploading the certificate, if necessary, you can download the public key certificate for distribution to your endpoints.

Generating a Self-Signed Delinea Connector IWA Host Certificate

1. Run the script below as an administrator on the server running the Delinea Connector.
2. Change the file path to the desired location.
3. Copy and save the password.

```
$domain_name = $env:userdnsdomain;  
    $dns_name = $env:computername + '.' + $domain_name;  
    $date_now = Get-Date;  
    $extended_date = $date_now.AddYears(3);  
    $user = $env:userprofile  
    $mycert=New-SelfSignedCertificate -DnsName $dns_name -CertStoreLocation  
cert:/LocalMachine/My -NotAfter $extended_date;$mycert  
    $pass = Read-Host 'what is your password?' -AsSecureString;  
    Export-PfxCertificate -Cert $mycert -FilePath $user\Desktop\cert-  
selfsigned.pfx -Password $pass
```

4. Click **Settings** from the left navigation, then click **Connectors**.
5. Click the name of the machine where Delinea Connector is installed.
6. Select the **IWA service** tab, then click **Edit**.
7. In **DNS hostname**, enter the FQDN of the Connector machine.
8. In **IWA detection timeout**, accept the default value or provide your desired value.
9. In the **HTTPS port number** field, enter **8443**. For MFA on PCS, endpoints that need to do MFA must be able to contact the Connector on 8443 and 8080.
10. In *Connector host certificate*, click **Upload certificate**.
11. Click **Select file**.
12. Browse to and select the host certificate file (.pfx or .p12 formats are supported).
13. Click **Open**.
14. Enter the password you used when running the PowerShell script to generate the certificate.
15. Click **Save**.
16. Click **Edit** again.
17. Next to Web Server, select **Enabled**.
18. Click **Save**.
19. You must restart the Delinea Connector after importing the certificate.



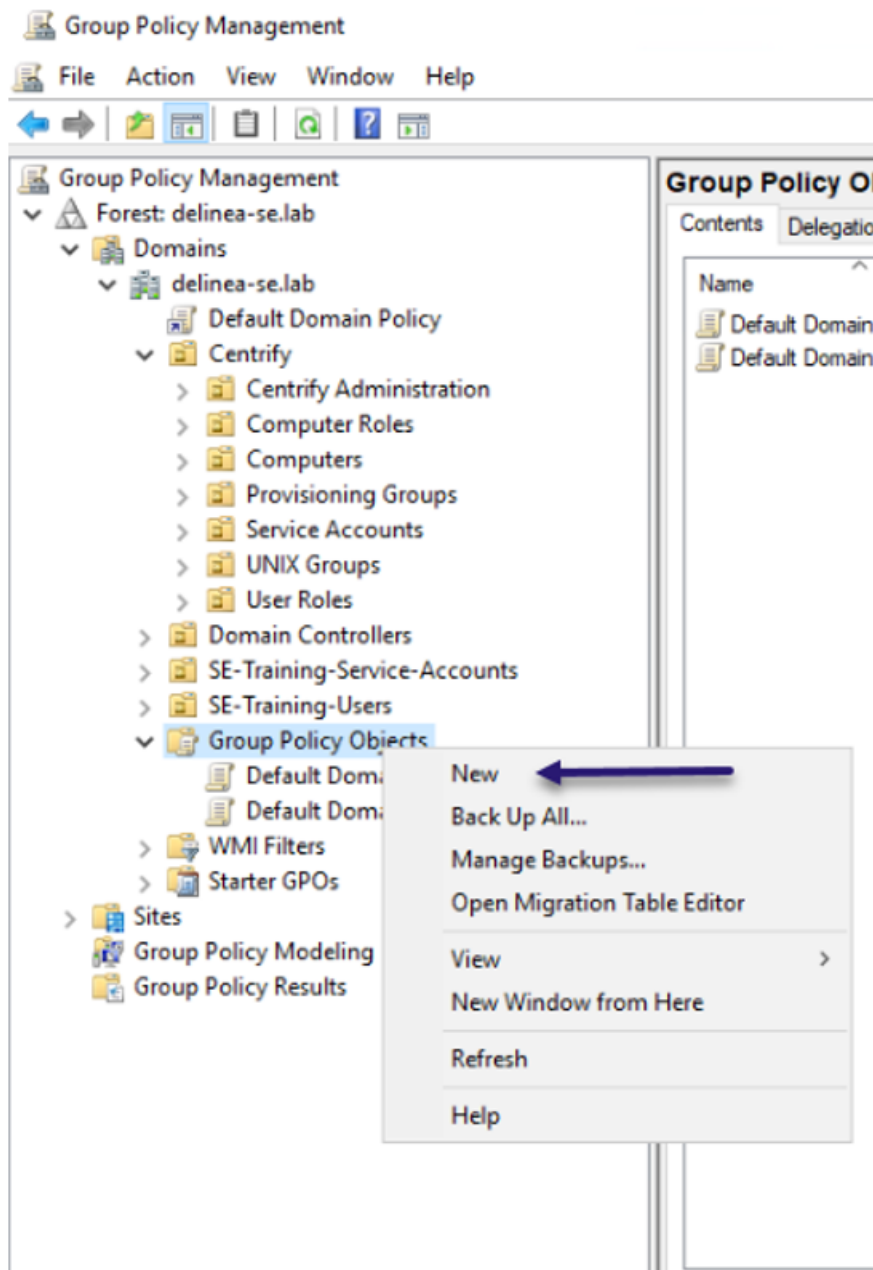
Note: Click the following link if you wish to "Setting Up a Certificate for Internal MS CA" on page 624.

Downloading the Delinea Connector IWA Host Certificate

1. If you are not already on the connector detail page, click Settings from the left navigation, then click Connectors. and click the name of the machine where Delinea Connector is installed.
2. Click the **IWA service** tab.
3. In Public key certificate, click **Download root certificate** to download the Connector host certificate.
4. Click the **Agent proxy** tab and verify that the agent is enabled on the proxy server.

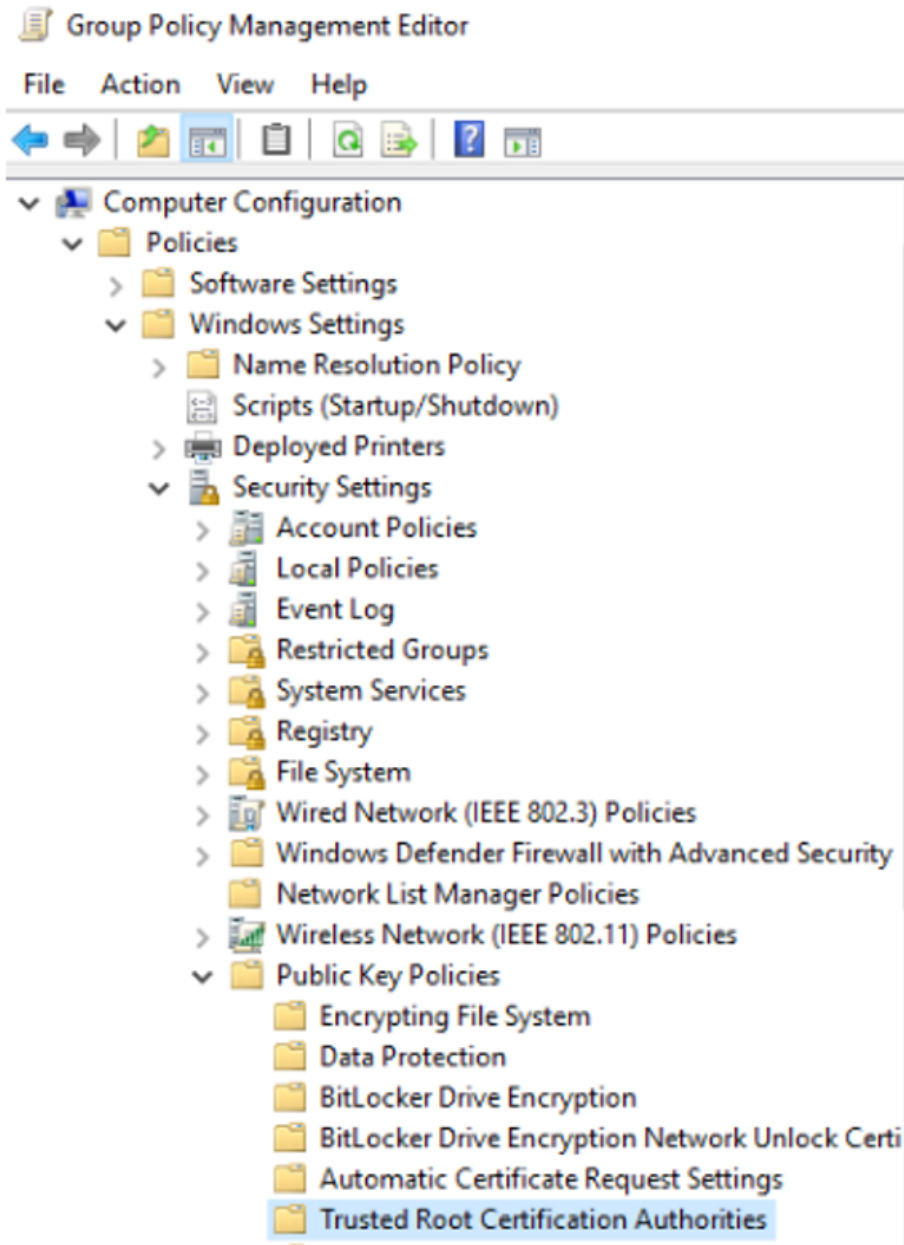
Distributing the Delinea Connector IWA Host Certificate for Agent Installation

1. On the host server, open **Group Policy Management** (Start > Run > `gpmc.msc`).
2. Refer to the example screen shot to perform the tasks below it:



3. Expand the forest (for example, delinea-se.lab).
4. Expand the domain (for example, delinea-se.lab).
5. Right click **Group Policy Objects**, and select **New**.
6. In the New GPO dialog, enter a name.
7. Click **OK**.
8. Right-click the name of the GPO you just created, and select **Edit**.

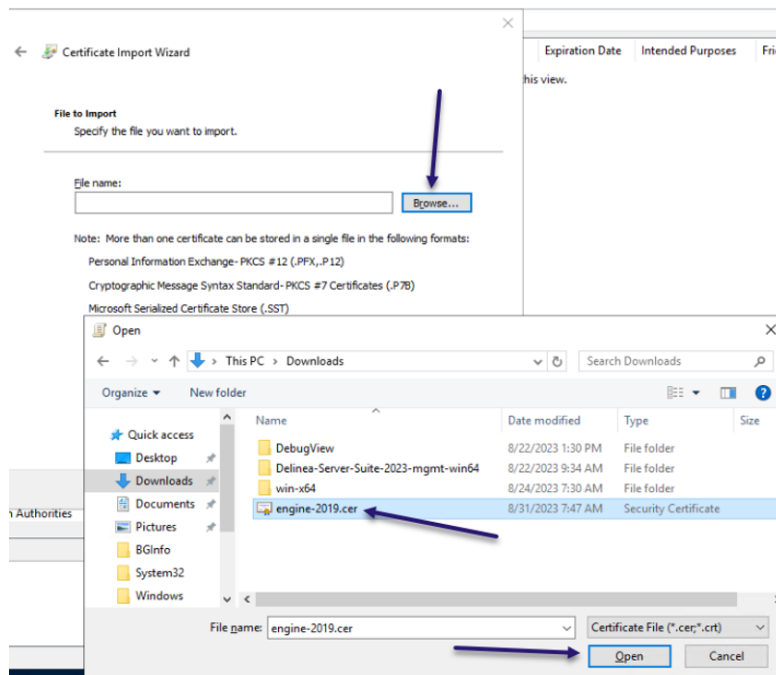
9. On the host machine, open the **Group Policy Management Editor**.
10. Select **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.



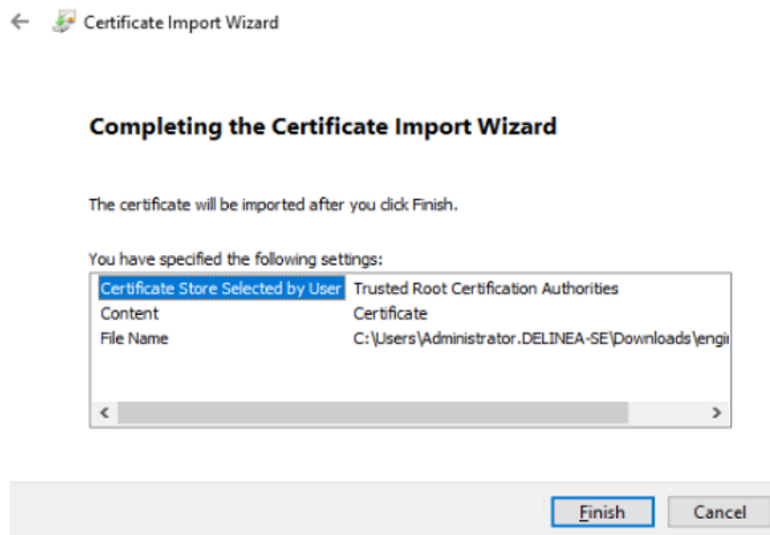
11. Right-click **Trusted Root Certification Authorities** and select **Import**.
The Welcome screen opens to the Certificate Import Wizard.
12. Click **Next**.
13. For File to Import, click **Browse**.

Multi-Factor Authentication

- Click the filename of the host certificate you downloaded earlier.



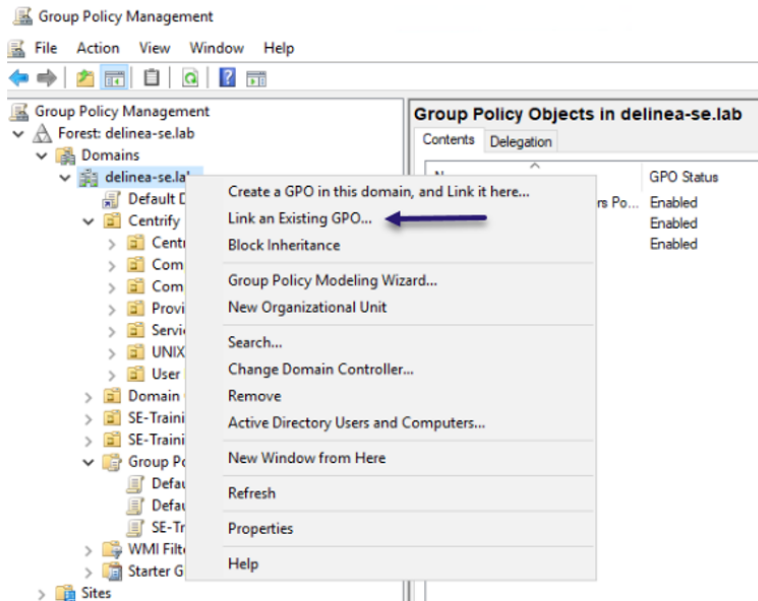
- Click **Open**.
- Click **Next**.
- Be sure that you see Trusted Root Certification Authorities in *Certificate Store Selected by User*.



- Click **Next**.
- Click **Finish**.

Multi-Factor Authentication

20. Wait for the Certificate Import Wizard to appear.
21. Click **OK**.
22. Close the Group Policy Management Editor.
23. In Group Policy Management, right-click the domain you created.
24. Select **Link an Existing GPO...**

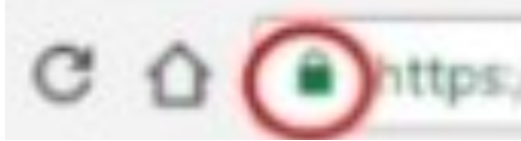


25. Select the IWA Host Certificate.
26. Click **OK**.

Verifying IWA Over HTTPS

You can test the validity of the Delinea Connector host certificate as follows:

1. Open a web browser from an endpoint machine.
2. Navigate to the following address:
`https://<connector_hostname>:<https_port>/iwa/sitecheck.`
3. Replace `<connector_hostname>` and `<https_port>` with the corresponding values. For example:
`https://2019WindowsServer:8443/iwa/sitecheck.`
4. Look in the browser navigation bar for an indication that the connection is secure. This appears differently depending on your browser. In some browsers, a green padlock icon appears. In other browsers, a different icon appears in this location, which you can click to get the security status.



If the browser indicates that the connection is secure, and the page opens and shows "result": "success" followed by the token, IWA is verified. The IWA service on the Delinea Connector, and the Identity Policy setting allowing the use of IWA, are both enabled and working.

Troubleshooting:

- If the page does not open, IWA service on the Delinea Connector might be disabled. To enable it, use the IWA Settings tab in the Connector page. Also check the IWA Settings tab in the Identity Policy page to be sure IWA is enabled.
- If the page opens but shows a result that is not "success," the Identity Policy setting for the use of IWA connections might be disabled. To enable it, use the IWA Settings tab on the Identity Policy page.
- If the page opens with an SSL or security error, the Connector certificate might not be fully configured. Make sure the certificate has been imported to the Trusted Root Certification Authorities, as described in "Distributing the Delinea Connector IWA Host Certificate for Agent Installation" on page 510.

Allowing IWA Connections for Users in the Default Policy

You can configure the platform to bypass already configured authentication rules and default authentication profiles when IWA is configured.

1. Click **Access** from the left navigation, then select **Identity Policies**.
2. Click to open the Default Policy.
3. Select the **Authentication** tab.
4. Scroll to Other Settings. Confirm that all three options for IWA connections are selected. If not, click **Edit** and set them:
 - **Allow IWA connections:** Required. Configures the platform to bypass already-configured authentication rules and default authentication profiles when IWA is configured.
 - **Set Identity Cookie for IWA Connections:** Optional. When you enable IWA, the platform can write a cookie in the current browser after a successful IWA-based log in. The platform checks the browser for this cookie when the user logs in to the platform. As long as the cookie is there, the user is not prompted for multi-factor authentication.
 - **IWA Connections satisfy all MFA mechanisms:** Optional. This option tells the platform to allow IWA to override all application specific authentication requirements.
5. Click **Save**.

Using IWA With Identity Cookie

This is an optional configuration. When you enable Integrated Windows Authentication (IWA), the platform can write a cookie in the current browser after a successful IWA-based login. The platform checks the browser for this cookie when the user logs in. As long as the cookie is there, the user is not prompted for multi-factor authentication.

To use IWA with identity cookie:

Multi-Factor Authentication

1. Click **Access** from the left navigation, then select **Identity Policies**.
2. Click an identity policy to open it.
3. Select the **Authentication** tab.
4. Scroll down to Other Settings and select the **Set identity cookie for IWA connections** checkbox. This option tells the platform to write a cookie in the current browser after a successful IWA-based log in.
5. Click **Save**.

Using IWA to Authenticate Application Access

Perform the procedure below if you want to enable the IWA connections satisfy all MFA mechanisms policy, which allows IWA to override all application-specific authentication requirements. In situations where additional step-up MFA challenges must normally be satisfied to access an application, no additional challenges are presented as long as the allotted pass-through duration has not expired.

To allow IWA for applications that require authentication:

1. Click **Access** from the left navigation, then select **Identity Policies**.
2. Click an identity policy to open it.
3. Select the **Authentication** tab.
4. Scroll down to Other Settings and select the **IWA connections satisfy all MFA mechanisms** checkbox. With this option, the platform allows IWA to override all application specific authentication requirements.
5. Click **Save**.

Disabling IWA

IWA is not required for manual authentication using the platform. If you cannot use IWA on the corporate network, you can disable it.

To disable Integrated Windows Authentication:

1. Click **Settings** from the left navigation, then select **Connectors**.
2. Click the name of the machine where Delinea Connector is installed.
3. Select the IWA Service tab and click **Edit**.
4. In Web Server, deselect the **Enabled** checkbox.
5. Click **OK**.

Configuring OTP Client Authentication

Organizations can enhance security by implementing OATH OTP-based authentication alongside standard password-based login for local Delinea Platform accounts.

This topic outlines the steps to enable users to enroll and log in to the Delinea Platform using an OTP client as a Multi-Factor Authentication (MFA) mechanism.

The same approach can be extended to users from external directories, such as Active Directory (AD), though some additional configuration may be required. The platform's identity policies and authentication profiles provide

extensive flexibility, enabling organizations to design authentication workflows that meet their specific security and operational needs—going beyond the basic setup described in this topic.

Create a Group for OTP Users

1. Navigate to **Access > Groups**.
2. Click **Add Group** and provide a name (e.g., OTP-group).

Define an Identity Policy for OTP Authentication

An identity policy enforces authentication rules for users. Configure an OTP-based identity policy and assign it to the group.

1. Navigate to **Access > Identity policies**.
2. Click **Add Policy** and provide a name (e.g., OTP-policy).
3. Assign the identity policy to the group (e.g., OTP-group).
4. At a minimum, configure the policy with the following settings:
 - a. Navigate to the **Authentication** tab.
 - i. In the **Services** section, click **Edit**.
 - ii. Select **Enable authentication policy controls**.
 - iii. Set (or create) a **Default authentication profile** with the following authentication mechanisms:
 - Challenge 1: Password
 - Challenge 2: OATH OTP client
 - iv. Click **Save**.
 - b. Under **Other Settings**, click **Edit**.
 - i. Enable **Allow users without a valid authentication factor to log in** and **Save**. **NOTE on using MFA with OATH OTP for new users:** This setting is not enabled by default, but it must be enabled to allow new users to access the platform to set up their second authentication challenge. If this setting is not enabled, new users will be advised that they need an additional authentication challenge to log in.
 - c. Under **User Security > OATH OTP** tab, click **Edit**.
 - i. Enable **OATH OTP integration** to allow users to authenticate using an OTP client, and **Save**.
 - d. Under **User Security > Authentication settings**, click **Edit**.
 - i. Enable **Enable users to configure an OATH OTP client** (requires enabling OATH OTP policy).
 - ii. Enable **Require users to configure at sign-in**. This forces users to enroll their OTP client during onboarding before gaining full access to the Platform.
 - iii. Specify an OATH OTP Display Name (e.g., Google Authenticator).

Multi-Factor Authentication

iv. **Save.**

Enable users to configure an OATH OTP client (requires enabling OATH OTP policy)

This policy is typically used when you bulk upload OATH tokens (for example, those generated by a YubiKey). Enable this option to display the QR code to users. Disable it to hide the QR code from users. The "Not Set" status here is equivalent to "Enabled".

Enabled	
Require users to configure at sign in	Enabled
OATH OTP display name	Google Authenticator
Authentication profile required to configure OATH OTP client	Not Set

Create and Onboard an OTP User

Once the identity policy is set up, create a test user and verify the onboarding flow.

1. Create a local user (e.g., OTP-user@domain).
2. Assign the user to the OTP user group (e.g., OTP-group).
3. The user will receive an invitation email to join the Delinea Platform.
4. After accepting the invitation, the user will be required to set a password during their first log-in.
5. The user will then be prompted to enroll their OTP client (e.g., Google Authenticator).

Additional authentication

To continue, you need to set up additional authentication method(s) for accessing the Delinea Platform.

Optional

Security questions

Click to configure

Required

Google Authenticator

Click to configure

Optional

Fido2

Click to configure

Optional

On-device authenticator

Click to configure

CLOSE

CONTINUE

6. The user will scan the QR code generated by the platform and follow the steps provided to complete the

Multi-Factor Authentication

enrollment.

Configure Google Authenticator

1. Install your third-party authenticator app.
2. Launch your authenticator app and tap the "+" icon or "Add Account" button to add a new account.
3. Select "Scan Barcode" or "Scan QR Code" and use your phone's camera to scan this code.
4. Enter the 6 digit code generated by your authenticator app.



Code *

Cancel

Verify

Platform Login Flow

Next time the user tries to login to platform they will follow these steps:

1. Enter their username and password.
2. When prompted, enter the **OTP code** generated by their OTP client (e.g., Google Authenticator).
3. If authentication is successful, access to the Delinea Platform is granted.

Summary

By implementing OATH OTP-based authentication, users benefit from an additional layer of security while ensuring seamless access management. This approach helps organizations enforce MFA best practices, reducing the risk of unauthorized access to the Platform.

Contractor and Vendor Access

Organizations can use membership types in the Delinea Platform to manage user entitlements between limited Vendor User capabilities and full-featured IT User capabilities in Secret Server. The following table shows the differences between these two types of entitlements.

Delinea Platform users are automatically granted IT User entitlements unless their membership type is explicitly set to "Vendor".

Capability	Vendor User	IT User
View secrets	✓ (Passwords are invisible)	✓
Launch secrets	✓ (PRA)	✓
Request access to secrets	✓	✓

Capability	Vendor User	IT User
Approve access to secrets		✓
Share secrets		✓
Create and manage secret and folder lifecycle		✓
View secret and user audit logs for owned secrets		✓
Use Connection Manager to login to Secret Server		✓
Use the Secret Server SDK and API		✓
Configure security features for a secret		✓
Configure password rotation		✓
All administrative functions in Secret Server		✓
Create/Manage Integrations, Workflows, Pipelines, Discovery, Sites. Distributed Engines, HA/DR, etc.		✓



Note: Customers who have purchased PRA concurrent user licenses are entitled to Vendor User capabilities automatically. Learn more about PRA ["Understanding PRA Entitlements "](#) on page 357.



Important: Entitlements are enforced even if a user is granted RBAC permissions for related actions.

Prerequisites

If you are using Secret Server On-Premise with the Delinea Platform, see ["Connecting to Secret Server On Premise"](#) on page 796 for the currently supported version.

Local Users

Customers can use their Delinea Platform local directory to onboard third-party users who need short-term access. Customers can also use the local directory when they do not want to add third-party users to their own identity sources. For details, see [Adding a Local User Account](#).

Bulk Import of Vendors

Delinea Platform provides a bulk import capability for organizations that deal with large numbers of third-party users and need an efficient way to manage access to Secret Server entitlements. To use bulk import, you prepare a file with user data, format it according to the system's requirements, and upload it.

For more detailed information about importing vendors in bulk, see ["Bulk Importing Local Users"](#) on page 173.

Active Directory

Tenant administrators can manage third-party vendor entitlements through Active Directory. For more information, see ["Managing Vendor Entitlements with Active Directory"](#) on the next page.

Federated Vendors

Tenant administrators must create a custom attribute in the identity provider (IdP) and map it to a *PlatformUserMembershipType* claim in the Delinea Platform. Claims for users must have a value of either **Vendor** or **Employee**.

For more information about managing third parties from a federated identity source using SAML or OIDC, see "SAML and OIDC Federation" on page 369.

Managing Vendor Entitlements with Active Directory

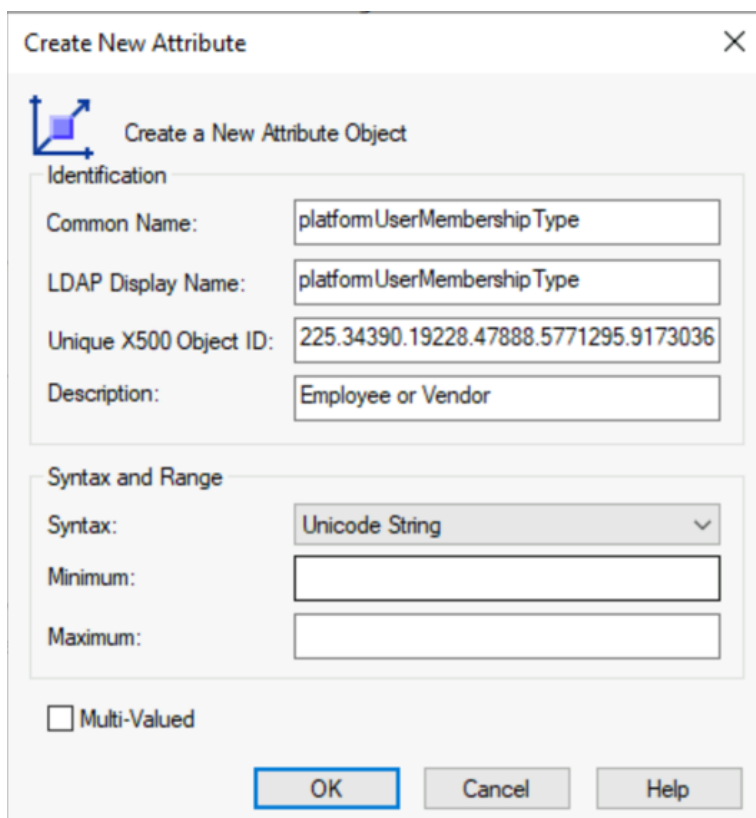
When third-party vendors want to use Active Directory with the Delinea Connector to log in to the Delinea Platform, you must make the following changes to ensure that these third-party vendors can be granted the appropriate entitlements in Secret Server. (For more information about the Connector, see "Active Directory Connector" on page 271.)

Notes:


- **Permissions:** Ensure you have the necessary permissions to modify user attributes and schema changes.
- **Replication:** Be aware of Active Directory replication delays if you're working in a multi-domain controller environment.
- **Testing:** Always test schema changes in a development environment before applying them in production.
- When the user logs in to the Delinea Platform, they will be granted appropriate third-party vendor entitlements.

To make user attribute and schema changes to ensure that third-party vendors can be granted the appropriate entitlements in Secret Server:

1. Open the Active Directory Schema Console.
 - i. Open a Command Prompt as an administrator.
 - ii. Type `regsvr32 schmmgmt.dll` and press **Enter** to register the Schema Management console.
 - iii. Type `mmc` and press **Enter** to open the Microsoft Management Console (MMC).
 - iv. In the MMC, choose **File > Add/Remove Snap-in**.
 - v. Select **Active Directory Schema** and click **Add**, then click **OK**.
2. Create an Attribute:
 - i. In the Active Directory Schema console, right-click on **Attributes** and select **Create Attribute**.
 - ii. A prompt is displayed, warning that you cannot delete the attribute once it is created. Click **Continue**.
 - iii. Create a new custom attribute named `platformUserMembershipType`. Fill in the required fields: Common Name, LDAP Display Name, and OID.

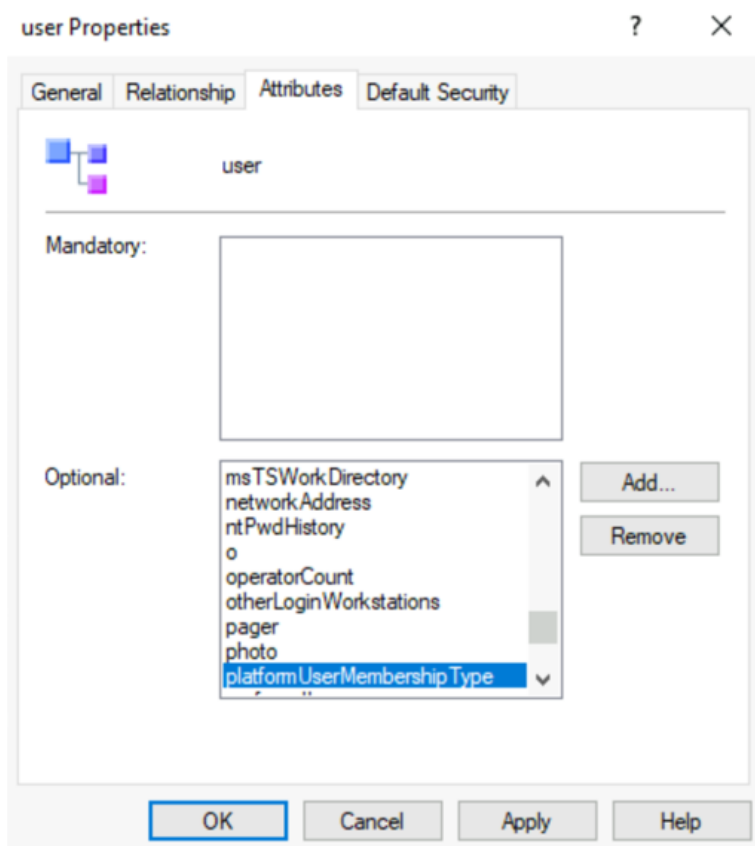


The screenshot shows the 'Create New Attribute' dialog box. It has a title bar with 'Create New Attribute' and a close button. Below the title bar is a section titled 'Create a New Attribute Object' with a blue icon. The dialog is divided into two main sections: 'Identification' and 'Syntax and Range'. The 'Identification' section contains four text boxes: 'Common Name' (platformUserMembershipType), 'LDAP Display Name' (platformUserMembershipType), 'Unique X500 Object ID' (225.34390.19228.47888.5771295.9173036), and 'Description' (Employee or Vendor). The 'Syntax and Range' section contains a 'Syntax' dropdown menu (Unicode String), and two empty text boxes for 'Minimum' and 'Maximum'. At the bottom of the dialog is a checkbox labeled 'Multi-Valued' which is unchecked. There are three buttons at the bottom: 'OK', 'Cancel', and 'Help'.

 **Note:** Ensure you have a unique X500 Object identifier for the attribute that is appropriate for your Active Directory. For more information, see [Obtaining an Object Identifier from Microsoft](#) on the Microsoft learning portal.

3. Add an Attribute Class:
 - i. Navigate to **Classes** in the Active Directory Schema console.
 - ii. Find and right-click the user and select **Properties**.
 - iii. Choose the **Attributes** tab and click **Add**.

- iv. Select the newly created attribute from the list and click **OK**.



4. Assign the Custom Attribute to a User:

After defining the custom attribute, you can assign it to users using tools like PowerShell or Active Directory Users and Computers (ADUC).

Using PowerShell:

To set a custom attribute for a user with PowerShell, use the following command:

PowerShell

```
Set-ADUser -Identity $username -Add @{$attributeName = $attributeValue}
```

Example: To add custom attribute `platformUserMembershipType` to the user `jdoe` and assign it a value of `vendor`:

```
Set-ADUser -Identity "jdoe" -Add @{platformUserMembershipType = "vendor"}
```

To update the value for the attribute, use the `-Replace` parameter instead of `-Add`:

Multi-Factor Authentication

```
Set-ADUser -Identity $username -Replace @{$attributeName = $attributeValue }
```

Example: To update the custom attribute `platformUserMembershipType` to a user `jdoe` and assign it a value of `employee`:

```
Set-ADUser -Identity "jdoe" -Replace @{platformUserMembershipType = "employee"}
```

Using Active Directory Users and Computers:

- i. Open Active Directory Users and Computers from the Administrative Tools.
- ii. Click on **View** and select **Advanced Features**.
- iii. Edit User Properties:
 - Find the user, right-click, and select **Properties**.
 - Choose the **Attribute Editor** tab.
 - Locate your custom attribute and enter the desired value.
- iv. Click **OK** or **Apply** to save the changes.

Notes:

- **Permissions:** Ensure you have the necessary permissions to modify user attributes and schema changes.
- **Replication:** Be aware of Active Directory replication delays if you're working in a multi-domain controller environment.
- **Testing:** Always test schema changes in a development environment before applying them in production.
- When the user logs in to the Delinea Platform, they will be granted appropriate third-party vendor entitlements.

Managing Vendor Entitlements with Federation

How to get an additional claim with OIDC federation (including Native EntraID integration).

Requirements

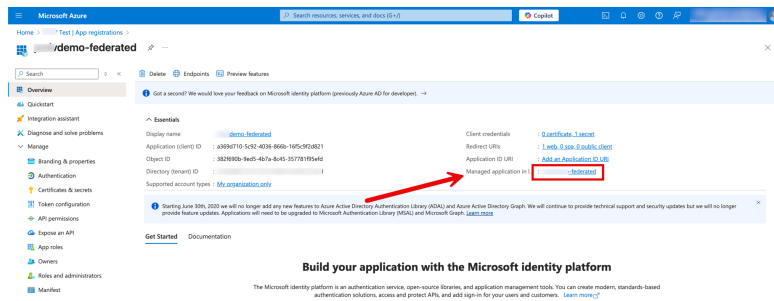
- A configured Delinea Platform
- Working OIDC based federation
- This can be either "plain" OIDC or Native EntraID integration which is based on OIDC.
- An attribute which one would like to map. This can be either an existing property available for claims mapping or a custom property defined in Entra. This is however out of scope of this document.
- For demonstration purposes, the user property called `department` will be used.

Adding a New Claim to EntraID App Registration

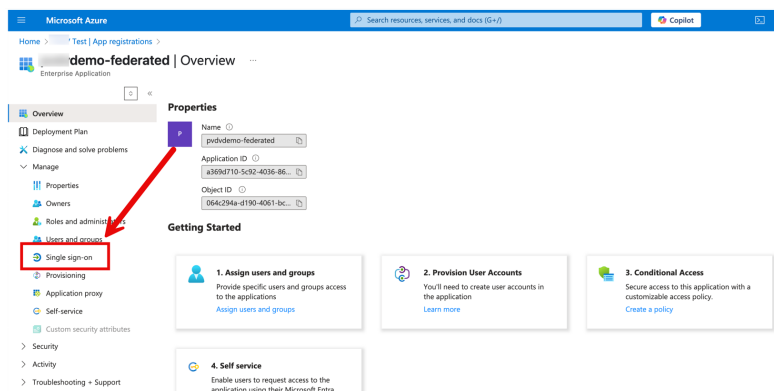
Unlike SAML-based federation, adding a new claim using OIDC-based federation is not actually configured on the app registration, but on the Enterprise App corresponding to the App Registration.

Multi-Factor Authentication

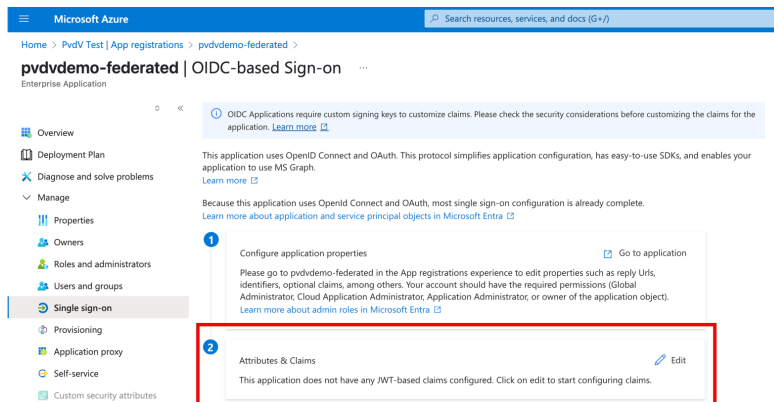
1. In Entra ID, browse to the App Registration that is used for the OIDC integration.
2. Navigate to the corresponding Enterprise App labeled as Managed application as shown.



3. When on the Enterprise Application page, select Single Sign-On from the menu on the left.



4. This should now allow for adding additional claims by selecting Edit on the Attributes and Claims section.



5. Select to add a new Claim.

Multi-Factor Authentication

Microsoft Azure

Home > Attributes & Claims

+ Add new claim + Add a group claim Columns Got feedback?

OIDC Applications require custom signing keys to customize claims. Please check the security considerations before customizing the claims for the application. [Learn more](#).

Required claim

Claim name	Type	Value
No claims configured		

Additional claims

Claim name	Type	Value
No claims configured		

6. Give the claim a name, this name is important to note down, as this will be the claim name which will be send to Delinea Platform and needs to have the value of Vendor or Employee.
7. In the example below, the name will be VendorType.

Microsoft Azure

Home > Attributes & Claims > Manage claim

Save Discard changes Got feedback?

Name * VendorType

Namespace Enter a namespace URI

Choose name format

Source * ☒ Attribute ☐ Transformation ☐ Directory schema extension

Source attribute * user.department

Claim conditions

Advanced SAML claims options

8. User.department in the example above, is a build-in field which also can be modified through the user properties page in EntraID. Note: Not all fields on the user properties page can be used as claims. One can also create custom properties / attributes but as per start of this document, this is out of scope of this document.
9. Following saving the new claim, the single sign on page of the enterprise app should now show this claim.

Microsoft Azure

Home > Test | Enterprise applications > Enterprise applications | All applications > -federated

-federated | OIDC-based Sign-on

Enterprise Application

Overview

Deployment Plan

Diagnose and solve problems

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service
- Custom security attributes

OIDC Applications require custom signing keys to customize claims. Please check the security considerations before customizing the claims for the application. [Learn more](#).

This application uses OpenID Connect and OAuth. This protocol simplifies application configuration, has easy-to-use SDKs, and enables your application to use MS Graph. [Learn more](#).

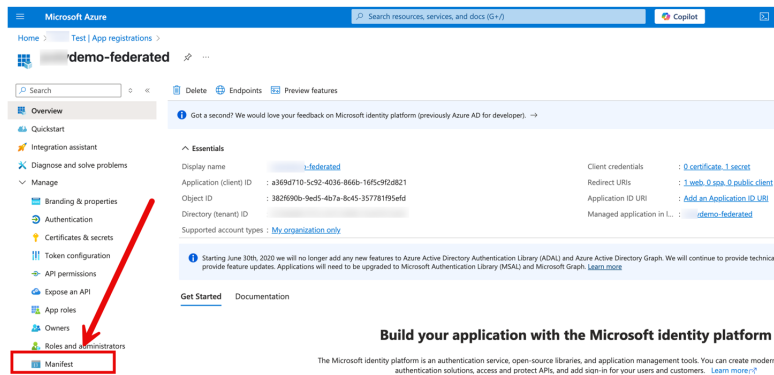
Because this application uses OpenID Connect and OAuth, most single sign-on configuration is already complete. [Learn more about application and service principal objects in Microsoft Entra](#).

1. Configure application properties. Please go to pvtvdemo-federated in the App registrations experience to edit properties such as reply Url, identifiers, optional claims, among others. Your account should have the required permissions (Global Administrator, Cloud Application Administrator, Application Administrator, or owner of the application object). [Learn more about admin roles in Microsoft Entra](#). [Go to application](#)
2. Attributes & Claims

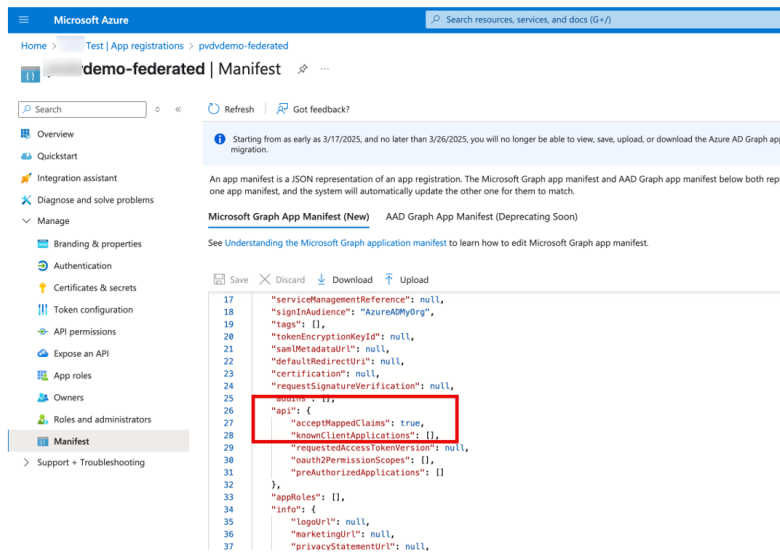
VendorType	user.department	Edit
------------	-----------------	------

Multi-Factor Authentication

- Now that the claim exists, the app registration needs to be reconfigured to allow mapped claims to be included in the response, as by default this is not allowed.
- To configure this, browse back to the app registration and select the Manifest option in the menu.



- In the manifest document, find the parameter: `acceptMappedClaims` and set the value to `true`.



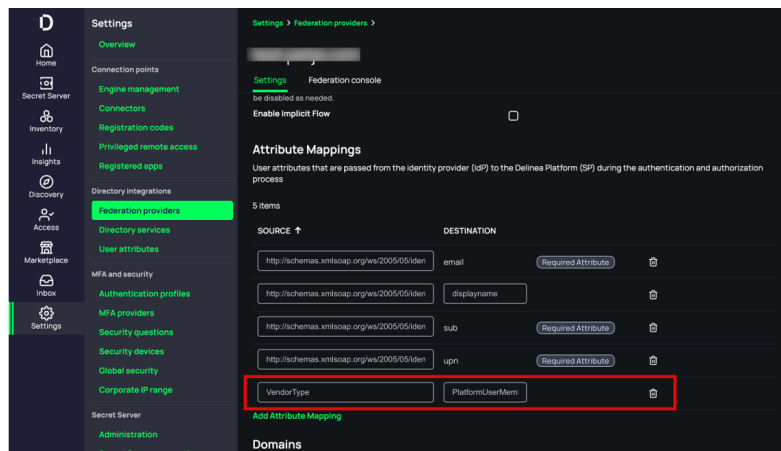
- This concludes the configuration required on EntraID side. Now to reconfigure Delinea Platform to map the incoming claim to the correct field in Platform.

Configuring Attribute Mappings in Delinea Platform

- Login to Delinea Platform and locate the federation settings under Settings > Federation Providers.
- Select the respective federation provider to enter the configuration of this federation provider.
- Select the edit button in the top right corner
- Scroll down to Attribute Mappings and add an Attribute Mapping
- The source field needs to match the Claim Name configured in the earlier step, in the example provided we used the name: VendorType

Multi-Factor Authentication

6. The Destination field name needs to be: PlatformUserMembershipType
7. This results in a configuration like the following:



8. Store the configuration by clicking the save button.

MFA Providers

Set up Multi-factor Authentication (MFA) providers for your tenant. Configuring MFA providers adds an additional layer of security to ensure that users accessing the Delinea Platform are properly authenticated. The Delinea Platform has integrated the following MFA providers:

- [Configuring Duo Authentication](#)
- [Configuring RADIUS Authentication](#)

Configuring Duo Authentication

This documentation is a detailed guide for setting up Duo authentication on the Delinea Platform.

The following procedures require copying and pasting information between Cisco Duo and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

For details on enabling MFA on the Delinea Platform, see [Identity Policies](#).

Prerequisites

- On the Delinea Platform, you will need to be a Platform Admin or have a role with the following permission: `delinea.platform/identity/admin/manage`
- In Duo, you must be an Administrator and have access to the Duo Admin Console where you can protect applications and create users.

Build a Duo Application

1. In the Duo Admin Console, navigate to **Applications**.
2. Select **Protect an Application**.



Multi-Factor Authentication

- 3. Filter the list of applications by entering web SDK.
- 4. In the Web SDK row, click **Protect**.

[Dashboard](#) > [Applications](#) > Protect an Application

Protect an Application

Web SDK

Application	Protection Type		
 Partner WebSDK	2FA	Documentation	<button>Protect</button>
 Web SDK	2FA	Documentation	<button>Protect</button>

- 5. Copy and save the **Client ID**, **Client secret**, and **API hostname**. You will need these to configure Duo authentication on the Delinea Platform.

[Dashboard](#) > [Applications](#) > Web SDK

Web SDK

[Authentication Log](#) |  [Remove Application](#)

See the [Duo Web SDK Documentation](#) to integrate Duo into your custom web application.

Details

[Reset Client Secret](#)

Client ID

Copy

Client secret

Copy

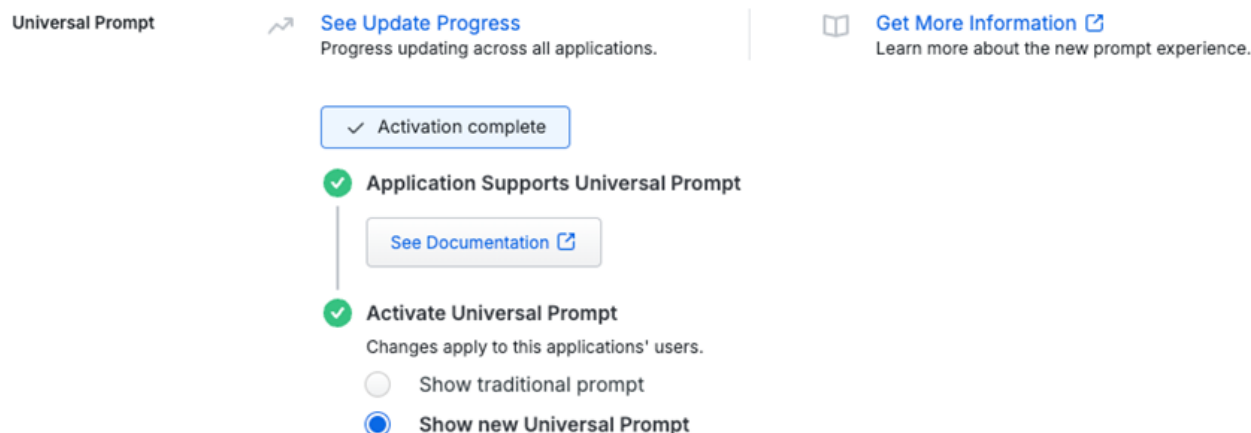
API hostname

Copy

Don't write down your client secret or share it with anyone.

Multi-Factor Authentication

- Under **Universal Prompt**, ensure that **Show new Universal Prompt** is selected.



Universal Prompt

[See Update Progress](#)
Progress updating across all applications.

[Get More Information](#)
Learn more about the new prompt experience.

✓ Activation complete

✓ Application Supports Universal Prompt
[See Documentation](#)

✓ Activate Universal Prompt
Changes apply to this applications' users.

☐ Show traditional prompt

☒ Show new Universal Prompt

- (Optional) Configure policies per your requirements. Also see "Duo Policies" on page 532 below.
- (Optional) Configure settings per your requirements. To enable self-service, see Duo's [Self-Service Portal](#) documentation.
- Navigate to the **Settings** section and update the **Name** field to something your users would recognize, like *Delinea Platform*.



Settings

Type Web SDK

Name

Duo Push users will see this when approving transactions.

- Click **Save**.

Add Duo to the Platform

Add Duo as an MFA Provider

- Log in to the Delinea Platform.
- From the left navigation menu, click **Settings**, then click **MFA Providers**.
- From the **Add Provider** button, select **Duo**.
- On the Add Duo page:
 - Enter a name.
 - Set the state to **Enabled** to activate the integration.
 - Enter the *API hostname* copied from Duo.

Multi-Factor Authentication

- d. Enter the *Client ID* copied from Duo.
 - e. Enter the *Client secret* copied from Duo.
5. Click **Add Provider**.

Add an Authentication Profile with Duo as an Authentication Challenge

For more information, see [Authentication Profiles](#).

1. From the left navigation menu, click **Settings**, then click **Authentication profiles**.
2. Click **Add Authentication Profile**.
3. Add a Profile name.
4. Under **Authentication challenges**, select **Duo** and other authentication challenges such as **Password**, as required.

Enable the Authentication Profile in an Identity Policy

For more information on identity policies and how to set up, edit, and assign them, see [Identity Policies](#).

1. From the left navigation menu, click **Access**, then click **Identity policies**.
2. Select the identity policy that should use Duo.
3. In the Overview section, if the policy is not Enabled, select **Edit**, set the state to **Enabled**, and **Save**.
4. Select **Authentication**.
5. Next to **Services**, click **Edit**.
6. Select **Enable authentication policy controls**.
7. Click **Default authentication profile**.
8. From the drop-down menu, select the authentication profile that has Duo configured as an authentication challenge.
9. Click **Save**.

For more information see [Authentication Profiles](#).

When using authentication rules in identity policies, these rules may override the default authentication profile. For more information, see the [Authentication Rules](#) documentation.

Enrolling Duo Users

You are now ready to invite users to use Duo as an authentication method.

1. In the Duo Admin Console, navigate to **Users**.
2. Select the desired user.
3. Click **Send Enrollment Email**. This action will send an email to the user with the necessary enrollment links. Users must complete enrollment with Duo to receive authentication challenges.



Important: When adding a user to Duo, make sure to use the same username and email address they use on the Delinea Platform.

Multi-Factor Authentication

For details on enrolling users, see the Duo documentation, [Duo Administration - Enroll Users](#).

For details on managing users, see the Duo documentation, [Duo Administrators - Manage Users](#).

Duo Policies

To prevent users who have not yet enrolled in Duo from accessing the Delinea Platform, set the New User Policy to **Deny Access**.

For details, see Duo's documentation on [Users Policy Settings](#).

Configuring RADIUS Authentication

You can use your RADIUS server to authenticate users to the Delinea Platform.

Radius Authentication Overview

To enable RADIUS authentication, use the following steps:

- Configuring a RADIUS Server
- Configuring the Delinea Connector as a RADIUS client
- Configuring an MFA profile and identity policy for RADIUS

Configuring a RADIUS Server

You must first configure your RADIUS server to recognize the Delinea Connector as a valid client. Your procedure may differ slightly depending on the RADIUS server you are using.

In most cases you need the following information, regardless of the RADIUS server you are using:

- Hostname or IP address of the Delinea Connector
- The secret key you provide to the RADIUS server and platform

To add and configure the RADIUS server:

1. Click **Settings** from the left navigation, then select **MFA Providers**.
2. Click **Add Provider**.
3. Enter the relevant information, according to the fields listed below:
4.
 - **Name**: This field is for the server name displayed to users as one of their MFA mechanism options.
 - **Hostname**: The server hostname or IP address.
 - **Port**: Port number (default: 1812).
 - **Server Secret**: The secret that is shared between the RADIUS Server and the Delinea Platform. If you have entered a secret key on your RADIUS server, enter that same key here. The keys must match to enable authentication. If you are creating a new secret key, best practices recommend 22 or more characters in length.
 - **Receive Timeout (seconds)**: Specify the receive timeout for this server. The value must be no less than 5 seconds and no greater than 55 seconds.

- **Enable silent initial request + Silent request answer:** Enable this option when the RADIUS server requires a fixed answer for the initial request.
For example, when using an RSA RADIUS Server with “Enable Only Additional Authentication,” the initial request to the server is sent with a username and whatever answer is specified in the **Silent request answer**.
- **User Identifier Attribute:** This specifies the user name format sent to the RADIUS client for authentication. You can select from the default list or define your own by selecting **Custom**.
 - **CanonicalName:** The CanonicalName default attribute is a computed value and is computed differently for each user type.
 - For Active Directory users, it is set to one of the following (in this order):
 - a. userPrincipalName - If the format is usable (not empty and does not start with “@”).
 - b. The concatenation of sAMAccountName, a “@”, and the AD domain.
 - For Delinea Platform users, as the contents of the Name field, the UUID default attribute represents the user ID stored on the platform.
 - **DistinguishedName:** This comes directly from the identity provider.
 - **Uuid:** This comes directly from the identity provider.
 - **EmailAddress:** This comes directly from the identity provider.
 - **Custom:** When you define a custom attribute, the named attribute must exactly match the user attribute name in the directory service. For example, you must use “sAMAccountName” instead of “sam account name” or “mail” instead of “Mail.”
- **Response Input Label:** This sets a custom label to use for the response input during login. This field can be up to 70 characters.

[Administration](#) > [Network](#) > [MFA Providers](#) >

My Radius Server

Integrate with MFA providers using RADIUS to allow for 3rd party RADIUS authentication for enhanced security

[Edit](#)

Name	My Radius Server
Description	None
Hostname	192.0.2.20
Port	1812
Server secret	*****
Receive timeout	5
Silent initial request	Disabled
User identifier attribute	CanonicalName
Response input label	None

5. Click **Add Provider**.

Configuring the Delinea Connector as a RADIUS Client

To configure the Delinea Connector as a RADIUS client, you need to update its RADIUS settings. To do this:

1. Click **Settings** from the left navigation, then select **Connectors**.
2. Select one of the connectors listed.
3. Click the **RADIUS Server** tab.

Administration > Network > Connectors >

My Connector

Summary IWA service **RADIUS server** Agent proxy

Delinea Platform allows the use of Remote Authentication Dial-In User Service (RADIUS) two-factor authentication as an Multi Factor Authentication option. The Delinea Connector acts as a RADIUS client that can communicate with any server implementing the RADIUS protocol. [Learn more about RADIUS support](#)

Edit

External radius servers

Enabled

Radius server secret override

Disabled

4. Click **Edit**.
5. Enable the option for **External RADIUS servers**.
6. (Optional) If you do not want all your Delinea Connectors to have the same shared secret, you can override the secret here and enter a different secret. To do so, select the option to enable **RADIUS server secret override**.
7. Click **Save**.



Note: Any change to Connector settings propagate from the platform to the Connector at an interval determined in the Connector settings under **Settings update interval**. See "Enabling Auto-Update for the Delinea Connector" on page 279.

Using Multiple Delinea Connectors as RADIUS Clients

If you have multiple Delinea Connectors enabled for use as RADIUS clients, the platform prioritizes connection with them in the following order:

1. Connectors from the same IP address as the user
2. If multiple Connectors are at the same IP address as the user, one is randomly chosen
3. The best subnet match will then be prioritized
4. If none of the above criteria are relevant, one is randomly chosen

Configure a RADIUS Authentication Profile

1. Click **Settings** from the left navigation, then select **Authentication profiles**.
2. Select an existing profile or add a new one.
3. Click **Edit**.

Multi-Factor Authentication

4. Enter a name and description.
5. **Challenge pass-through duration:** Select a duration from the dropdown list. The challenge pass-through duration allows people to stay logged in during that specified time period.
6. Select the authentication mechanisms for the profile. You must select **Third-party RADIUS authentication** as one of the mechanisms in at least one of the challenges.

For example:

Edit an authentication profile

Profile name *

RADIUS

Challenge pass-through duration

30 minutes

Authentication mechanisms

Challenge 1	Challenge 2 (optional)
<input checked="" type="checkbox"/> Password	<input type="checkbox"/> Password
<input type="checkbox"/> Mobile authenticator	<input type="checkbox"/> Mobile authenticator
<input type="checkbox"/> Phone call	<input type="checkbox"/> Phone call
<input type="checkbox"/> Text message (SMS) confirmation code	<input type="checkbox"/> Text message (SMS) confirmation code
<input type="checkbox"/> Email confirmation code	<input type="checkbox"/> Email confirmation code
<input type="checkbox"/> OATH OTP client	<input type="checkbox"/> OATH OTP client
<input type="checkbox"/> Third-party RADIUS authentication	<input checked="" type="checkbox"/> Third-party RADIUS authentication
<input type="checkbox"/> FIDO2 authenticator	<input type="checkbox"/> FIDO2 authenticator
<input type="checkbox"/> Slack confirmation code	<input type="checkbox"/> Slack confirmation code
<input type="checkbox"/> Security questions	<input type="checkbox"/> Security questions

Cancel

Save

Configure a RADIUS Identity Policy

You also need to configure an identity policy to control who can log in using RADIUS and how they must do so.

1. Click **Access** from the left navigation menu, then select **Identity policies**.
2. Select an existing policy, or add a new one and select it.
3. Select the **Authentication** tab.
4. Under Services, click **Edit**.
5. In **Enable authentication policy controls**, select **Enabled**.
6. In **Default authentication profile**, select the authentication profile you created earlier for RADIUS from the dropdown.

Multi-Factor Authentication

For example:

Administration > User Management > Policies >

My Radius Auth Policy

ConfigurationAuthenticationUser securitySummary

Services

Applies to all web logins to the cloud service, including the platform and on-demand application authentication. [Learn more about policies.](#)

Edit

Enable policy controls

Enabled

Default profile

RADIUS

Authentication Rules

Edit

Move up or move down rule to specify order. The highest priority is on top. If applicable, the rule displayed at the top of the table will be applied to the policy and will override the default profile.

0 items

RULE NAME

AUTHENTICATION PROFILE

No data found

- 7. Select the **User Security** tab.
- 8. Select the **RADIUS** sub-tab.
- 9. Click **Edit**.
- 10. In **Enable 3rd Party RADIUS authentication**, select **Enabled**.
- 11. Click **Save**.

Administration > User Management > Policies >

My Radius Auth Policy

ConfigurationAuthenticationUser securitySummary

Self servicePassword settingsOATH OTRADIOUSUser account settingsAuthentication settings

RADIUS client connections extend MFA to clients that support RADIUS.

Edit


Third-party RADIUS authentication

Enable third-party RADIUS authentication

Enabled

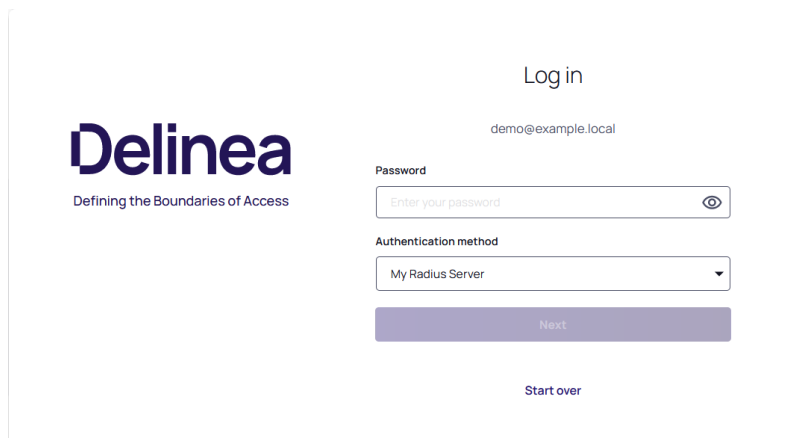
Using RADIUS Authentication

Users can access the Delinea Platform by opting for the RADIUS server authentication challenge method at the platform login prompt and then entering the passcode.

 **Important:** The passcode requirements may vary based on the specific authentication backend employed by the RADIUS server.

Registered Apps

For example, here's what it looks like at login when the service prompts a user to authenticate against the RADIUS server:



The screenshot shows the Delinea login page. On the left is the Delinea logo with the tagline "Defining the Boundaries of Access". The main heading is "Log in". Below it, the email "demo@example.local" is displayed. The "Password" section has a text input field with the placeholder "Enter your password" and a toggle icon. The "Authentication method" section has a dropdown menu currently showing "My Radius Server". Below these is a blue "Next" button. At the bottom, there is a "Start over" link.

Registered Apps

An application registration manages OAuth/OIDC integrations with other platforms. It enables the Delinea Platform to securely connect with third-party integrations such as Entra ID. This registration enables the platform to authenticate and interact with external systems, ensuring secure data and identity exchanges while maintaining high security and compliance standards.

- [Entra ID API Integration](#)
 - [Entra ID FAQs](#)

Entra ID API Integration

This documentation provides a detailed guide for integrating Entra ID with the Delinea Platform. The integration enables the Delinea Platform to use Microsoft APIs directly to access your Entra ID users and groups.

The integration supports the following:

- Log-in and authentication using Entra ID credentials.
- Browsing and searching for Entra ID users and security groups. Distribution lists (groups) are not supported.
- Direct use of Entra ID security groups on the platform without mapping them to platform groups.
- Pre-assignment of Entra ID users to groups, roles, identity policies, and sharing secrets.
- Inviting/adding Entra ID users directly to the platform.
- **New Feature:** User deactivation or deletion in Entra ID is reflected in the platform. This functionality was added with Public Preview.

Registered Apps

- **New Feature:** Easily manage which groups from Entra ID are visible and usable within the platform. This functionality was added with Public Preview. See [External Directory Group Allowlist](#).
- **New Feature:** Paginated results are returned when browsing Entra ID users and groups when managing role and identity policy member assignment and sharing secrets. This functionality was added with Public Preview.

This topic walks you through setting up an Entra ID API integration on the Delinea Platform. The platform provides two options for this integration. You only need to choose one of these methods:

- **Creating a Delinea-managed registered app.** This approach is recommended if you prefer to configure the Entra ID integration entirely within the Delinea Platform and let Delinea handle the creation and management of the necessary Azure components. **New Feature:** This functionality was added with Public Preview.
- **Creating a customer-managed registered app.** This approach is suitable if you prefer to maintain full control over the integration and manage the Azure resources yourself.

Prerequisites

- On the Delinea Platform, you must be a Platform Admin.
- In Azure, you must be able to create an app registration and manage API permissions. Roles that satisfy these requirements are:
 - Global Administrator
 - Privileged Role Administrator



Note: On the Delinea Platform, the Entra ID API Integration cannot run on the same Directory Tenant as [Entra ID Federation](#) or Active Directory (Connector), including implementations of Privilege Control for Servers. This misconfiguration would create potential collisions for an AD user sharing the same UPN (username or email address) as an Entra user, because each user has a unique Object ID (GUID).

Create a Delinea-Managed Registered App

This procedure walks you through setting up Entra ID on the Delinea Platform using a Delinea-managed registered app. To complete and test the integration you will need to do the following:

- Add a Delinea-managed registered app.
- Grant Delinea permission to create and manage application registrations in Azure.

Add a Delinea-Managed Registered App

1. On the Delinea Platform, navigate to **Settings > Registered apps**.
2. Click **Add App**.
3. Select **Delinea Managed Entra ID**.
4. On the *Add Delinea managed Entra ID App* page, complete the following fields:

Registered Apps

Delinea Platform Field	Description	Location in Azure App
Name	A unique identifier for the registered app in the Delinea Platform.	User-defined; choose a descriptive name when configuring in Delinea Platform.
Description	Optional field to add details or context about the registered app.	User-defined; optional entry in Delinea Platform.
Directory (tenant) ID	The unique identifier for your Azure AD tenant.	Found on the Azure App Registration → Overview page under "Directory (tenant) ID".

5. Select all settings in the table below:

Delinea Platform Field	Description
Entra ID - Read	Grants the platform the ability to query Entra ID users and groups. This permission is Azure tenant-wide and can only be granted once per platform tenant.
Log-in to Entra ID	Allows the creation of a Federation Provider within the Delinea Platform. This enables users to log in to the Delinea Platform using their Entra ID credentials. If needed, you can create multiple registered apps with Log-in permissions, each associated with a unique domain. When this option is selected, specifying the domains becomes mandatory.

6. Click **Save**.

Grant Delinea Permission to Create and Manage App Registrations in Azure

1. Grant Consent for the Delinea Entra ID Management App

- On the next screen in the *Entra ID app management* section, select **Grant consent**.
- In the *Microsoft Pick an account* dialog, log in with your Microsoft account credentials.
- In the *Permissions requested* dialog for Delinea Platform Azure Registered Apps:
 - Review the required permissions.
 - Select **Accept**.

2. Grant Consent to Read the Entra ID Users and Groups

Registered Apps

- a. In the *Entra ID - Read* section, select **Grant consent**.
 - b. In the *Microsoft Pick an account* dialog, log in with your Microsoft account credentials.
 - c. In the *Permissions requested* dialog for *Delinea Managed azure-entra-read*:
 - i. Review the required permissions.
 - ii. Select **Accept**.
3. **Select Domains for User Login**
- a. Click **Edit**.
 - b. In the *Log-in to Entra ID* section, select the desired domains for user login.
 - c. Click **Save**.
4. **Grant Consent to User Login**
- a. In the *Log-in to Entra ID* section click **Grant consent**.
 - b. In the *Microsoft Pick an account* dialog, log in with your Microsoft account credentials.
 - c. In the *Permissions requested* dialog for *Delinea Managed azure-entra-login*:
 - i. Review the required permissions.
 - ii. Select **Consent on behalf of your organization**.
 - iii. Click **Accept**.

After you have completed the steps above, the following three apps should be created in Azure and should reflect the state, **Consent granted** on the Delinea Platform:

- **Entra ID app management** (Delinea Platform Azure Registered Apps)
- **Entra ID - Read** (Delinea Managed azure-entra-read)
- **Log-in to Entra ID** (Delinea Managed azure-entra-login)

The Delinea Platform is now fully integrated with Entra ID, enabling a seamless, streamlined user management experience. You can now browse Entra ID users and groups directly on the platform, pre-assign permissions, add users instantly, and allow users to log in with their Entra ID credentials.

Create a Customer-Managed Registered App

This procedure walks you through setting up and testing Entra ID on the Delinea Platform using a customer-managed registered app.

1. **Register an App in Azure:**
 - a. **Generate a Client Secret:** Create a client secret, copy its value, and note the expiration date.
 - b. **Configure Token Claims:** Add the required claims for the Platform.
 - c. **Set API Permissions:** Assign the necessary Microsoft Graph permissions and grant admin consent.
2. **Register a customer-managed app on the Delinea Platform:** Enter the app credentials, permissions and domains.
3. **Test the Integration:** Verify the integration by logging into the Platform with an Entra ID user.



Note: The following procedures require copying and pasting information between Azure Portal and the Delinea Platform. We recommend opening both applications before you begin and keeping both open until you are finished.

Create an Azure Application Registration

1. Go to the Azure portal and log in.
2. Select (or search for) **App registrations**.
3. Click **New registration**.
4. In the **Name** field, enter a name for your application registration. (Under *Supported account types*, only *Single tenant* is supported).

[Home](#) > [App registrations](#) >

Register an application ...

* Name

The user-facing display name for this application (this can be changed later).

Delinea Platform Integration ✓

Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Delinea Identity Sandbox - Free only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼ e.g. <https://example.com/auth>

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

5. Click **Register**. The application registration's overview page opens.

Registered Apps

14. In the *Add optional claim* dialog, select **ID** under *Token type*.

Add optional claim

×

Once a token type is selected, you may choose from a list of available optional claims.

***Token type**
Access and ID tokens are used by applications for authentication. [Learn more](#)

☒ ID
☐ Access
☐ SAML

<input checked="" type="checkbox"/> Claim ↑↓	Description
<input type="checkbox"/> acct	User's account status in tenant
<input type="checkbox"/> acrs	Auth Context IDs of the operations the bearer is eligible t...
<input type="checkbox"/> auth_time	Time when the user last authenticated; See OpenID Conn...
<input type="checkbox"/> ctry	User's country/region
<input checked="" type="checkbox"/> email	The addressable email for this user, if the user has one
<input type="checkbox"/> family_name	Provides the last name, surname, or family name of the us...
<input type="checkbox"/> fwd	IP address
<input type="checkbox"/> given_name	Provides the first or "given" name of the user, as set on th...
<input type="checkbox"/> in_corp	Signals if the client is logging in from the corporate netw...
<input type="checkbox"/> ipaddr	The IP address the client logged in from
<input type="checkbox"/> login_hint	Login hint
<input type="checkbox"/> onprem_sid	On-premises security identifier
<input type="checkbox"/> preferred_username	Provides the preferred username claim, making it easier f...
<input type="checkbox"/> pwd_exp	The datetime at which the password expires
<input type="checkbox"/> pwd_url	A URL that the user can visit to change their password
<input type="checkbox"/> sid	Session ID, used for per-session user sign out
<input type="checkbox"/> tenant_ctry	Resource tenant's country/region
<input type="checkbox"/> tenant_region_scope	Region of the resource tenant
<input checked="" type="checkbox"/> upn	An identifier for the user that can be used with the userna...
<input type="checkbox"/> verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
<input type="checkbox"/> verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail
<input type="checkbox"/> vnet	VNET specifier information
<input type="checkbox"/> xms_cc	Whether the application can handle claims challenges
<input type="checkbox"/> xms_pdl	Preferred data location
<input type="checkbox"/> xms_pl	User-preferred language
<input type="checkbox"/> xms_tpl	Tenant-preferred language

Add Cancel

15. Select the following claims:

- email
- upn

16. Click **Add**.

Registered Apps

17. In the dialog box that opens, select **Turn on the Microsoft Graph email, profile permission (required for claims to appear in token)**.
18. Click **Add** to add the optional claims to the app registration token.

Optional claims

Optional claims are used to configure additional information which is returned in one or more tokens. [Learn more](#)

+ Add optional claim + Add groups claim

Claim ↑↓	Description	Token type ↑↓	Optional settings	
email	The addressable email for this user, if the user has one	ID	-	...
upn	An identifier for the user that can be used with the username_hint parameter; not a ...	ID	Default	...

19. From the left navigation menu, click **API Permissions**. API Permissions include all permissions required for the platform.
20. These three permissions will be on the **Configured permissions** list:
 - email
 - profile
 - User.Read

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission ✓ Grant admin consent for Delinea Identity Sandbox - Free

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (3)				
email	Delegated	View users' email address	No	...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user profile	No	...

21. Click **Add a permission**.
22. Click **Microsoft Graph**.
23. Click **Application permissions** and select the following:
 - Group.Read.All
 - GroupMember.Read.All
 - Member.Read.Hidden
 - User.Read.All
24. Click **Add permissions**.

Registered Apps

25. Click **Grant admin consent for <azure directory name>** for the API permissions you just added.

Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

+ Add a permission

✓ Grant admin consent for Delinea Identity Sandbox - Free

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (7)				...
email	Delegated	View users' email address	No	...
Group.Read.All	Application	Read all groups	Yes	⚠ Not granted for Delinea... ...
GroupMember.Read.All	Application	Read all group memberships	Yes	⚠ Not granted for Delinea... ...
Member.Read.Hidden	Application	Read all hidden memberships	Yes	⚠ Not granted for Delinea... ...
profile	Delegated	View users' basic profile	No	...
User.Read	Delegated	Sign in and read user profile	No	...
User.Read.All	Application	Read all users' full profiles	Yes	⚠ Not granted for Delinea... ...

26. In the *Grant admin consent confirmation* dialog, click **Yes**.
27. You are now ready to create a registered app on the Delinea Platform in the next section.

Create a Customer-Managed Registered App on the Delinea Platform

- On the Delinea Platform, navigate to **Settings > Registered apps**.
- Click **Add App**. Select **Customer Managed Entra ID**.

Registered Apps

3. On the *Add registered app* page, complete the following fields:

Delinea Platform Field	Description	Location in Azure App
Name	A unique identifier for the registered app in the Delinea Platform.	User-defined; choose a descriptive name when configuring in Delinea Platform.
Description	Optional field to add details or context about the registered app.	User-defined; optional entry in Delinea Platform.
Directory (tenant) ID	The unique identifier for your Azure AD tenant.	Found on the Azure App Registration → Overview page under "Directory (tenant) ID".
Application (client) ID	The unique identifier for the Azure app being registered.	Found on the Azure App Registration → Overview page under "Application (client) ID".
Client Secret Value	The value of the client secret generated for the app, used for authentication.	Generated in Azure App Registration → Certificates & Secrets. Copy the value immediately when creating the client secret.
Credential Expiration Date	The expiration date of the client secret used for authentication.	Found in Azure App Registration → Certificates & Secrets under "Expires". Match this value in Delinea Platform.

4. Select all settings in the table below:

Delinea Platform Field	Description
State	Indicates whether the integration is active. Ensure this is set to Enabled to allow seamless operation
Entra ID - Read	Grants the platform the ability to query Entra ID users and groups. This permission is Azure tenant-wide and can only be granted once per platform tenant.
Log-in to Entra ID	Allows the creation of a Federation Provider within the Delinea Platform. This enables users to log in to the Delinea Platform using their Entra ID credentials. If needed, you can create multiple registered apps with Log-in permissions, each associated with a unique domain. When this option is selected, specifying the domains becomes mandatory.
Provision Directory Services	This setting is required when creating the registered app, to ensure that the directory service and federation provider settings are created. This setting will be deprecated in future releases.

5. **Domain Names:** Add at least one domain, including the primary domain for your Microsoft Entra organization and any custom domains your users will use to log in.

Registered Apps

Registered apps >

MyApp [Preview](#)

Name * MyApp

Description My App

State ☒ Enabled

Directory (tenant) ID * 123456789-4272-b0eb-123456789
The unique identifier for your Entra ID directory (tenant)

Application (client) ID * 123456789-1e6c-403e-a001-123456789
The unique ID for your app in Entra ID

Client Secret Value * ***** [Show](#)
The client secret value associated with your app in Entra ID

Credential Expiration Date * 6/25/25 [Calendar](#)

API permissions * ☒ Entra ID - Read ☒ Log-in to Entra ID

Provision Directory Services ☒


Domain names * [Add](#)
Add the primary domain and any custom domains users log in with

1 item

DOMAIN NAME
example.com Remove

[Cancel](#) [Save](#)

6. Click **Save**.

 **Important:** Once the registered app is saved, the platform generates an OIDC federation configuration that can be viewed under **Settings > Federation Providers**, which gives Directory Services access to the Entra ID directory. To enable user login with Entra ID credentials, add the **Platform Callback URL** to the Azure app registration as described in the next section.

Update the Azure App Registration with the Platform Callback URL

Add the Platform Callback URL from the generated Federation configuration to the Azure app registration. The URL will be generated after you save the registered app.

1. On the Delinea Platform, navigate to **Settings > Registered apps**.
2. Select the registered app.
3. Copy the **Platform Callback URL**.
4. Navigate to the Azure portal.
5. From the app registration *Overview* page, select **Redirect URIs** and click **Add a Redirect URL**.
6. In the *Platform configurations* section, click **Add a platform**.
7. Select **Web**.
8. In the *Redirect URIs* field, enter the *Platform callback URL* that you copied and saved.
9. Click **Configure**.

The Delinea Platform is now fully integrated with Entra ID, enabling a seamless, streamlined user management experience. You can now browse Entra ID users and groups directly on the platform, pre-assign permissions, add users instantly, and allow users to log in with their Entra ID credentials.

Automating Entra ID Integration Setup

You may streamline the Entra ID provisioning process by leveraging the automation script available in the Delinea XPM GitHub repository. This script provides a simple and repeatable setup experience by automating the creation of the necessary Azure and Delinea Platform application objects. For more details and usage instructions, refer to the [Entra ID App Registration Automation Script](#) repository.

Test the API-Based Entra ID Integration

Create a test user in the Azure Portal and use the account to verify user login to the Delinea Platform.

1. Go to the [Azure portal](#) and log in.
2. Select or search for **Users**.
3. Click **New user > Create new user**.
4. Add the following:
 - User principal name
 - Display name
5. Copy the generated **Password** because you will need it to log on to the Delinea Platform.
6. Click **Next > Properties**.
7. Add Email.
8. Click **Review + create**.
9. Click **Create**.

Test User Log-on to the Delinea Platform

1. On the Delinea Platform, navigate to **Settings > Federation providers**.
2. Select the generated OIDC federation configuration.
3. Select **Federation console**.
4. Click **Start Debug Log**.
5. From a **private** browser window, navigate to your tenant and log on with the test user credentials.

The test user should be able to log on to the platform. If the user cannot log on, the Debug Log can help diagnose and resolve issues by capturing detailed information about the communication between the Platform and the Identity Provider (IdP). The log provides insights into federation messages, claims, and potential misconfigurations, making it easier to pinpoint errors or inconsistencies in the authentication process.

Entra ID FAQs

Can I use the Connector with the Entra ID API integration simultaneously?

The integration will fail if your platform tenant includes Active Directory (AD) users who share the same usernames or email addresses as Entra ID users or if AD and Entra ID manage the same domains. This setup creates identity collisions, since AD and Entra ID users with the same UPN will have different Object IDs (GUIDs). This applies to implementations of Privilege Control for Servers (PCS) and Server Suite, which both depend on Active Directory.

Can I use Entra ID Federation and Entra ID API integration simultaneously?

No. If your platform already has an Entra ID federation configuration, adding a new native Entra ID-registered app on the same Entra ID tenant will not succeed.

How is adding Entra ID users different from adding federated users?

While a federated user must log on to the platform once before their account appears on the platform, an Entra ID user can be added to the platform by an administrator and fully set up (with roles, permissions, groups, identity policies, secrets and folder sharing, etc.) before the Entra ID user first logs on to the platform. And unlike a federated group, an Entra ID group does not need to be mapped to a local group.

How is Entra ID Federation user mapping different from standard federation?

Standard federation supports user mapping to an Active Directory:

- The user object originates from AD
- Authentication occurs through federation
- Permissions can be assigned through AD users or groups, and MFA can also be set up for the user.

Entra ID federation configuration is system-generated and does not support user mapping to an Active Directory. This is a known, current limitation for Privilege Control for Servers, and we are actively working to address this limitation in future releases.

What if users can't log in after the integration is set up?

1. Ensure that the Registered App is "Enabled".
2. Verify that the API Permission, **Log-in to Entra ID** is selected for the registered app.
3. On the platform, navigate to **Settings > Federation providers** and select the Entra ID federation configuration.
4. Open the **Federation console** tab to run the debugging process.

What happens if I disable a registered app?

The registered app facilitates the connection between the Delinea Platform and Microsoft Entra ID. Disabling the registered app prevents Entra ID users from logging in to the Delinea Platform, and blocks administrators from querying the Entra ID directory.

Can I Create a Registered App for Each API Permission?

Yes, you may create a customer-managed registered app for each API permission as required.

What validations and errors might arise when creating a registered app?

Scenario: Attempting to create a registered app with the same "Log in to Entra ID" permission for an existing Entra ID application client ID.

- **Outcome:** A registered app cannot be created with duplicate permissions for the same application ID.
- **Message:** "An app '%appname' with 'Log in to Entra ID' permission already exists for client ID '%appclientid'."

Scenario: Attempting to register a platform app with "Read" permission for the same Entra ID tenant.

- **Outcome:** "Read" permission can only be granted once per Entra ID tenant, as it is tenant-wide.
- **Message:** "'Entra ID - Read' permission is already assigned to '%appname' for tenant '%tenantid'."

What customer-managed registered app configurations create different outcomes?

Entra ID - Read	Log-in to Entra ID	Provision Directory Services	Outcome
X	✓	✓	<ul style="list-style-type: none"> - Registration app created - Federation provider created - Entra ID users can log in to the platform.
✓	✓	✓	<ul style="list-style-type: none"> - Registration app created - Federation provider created - Directory service created - Entra ID users can log on to the platform - Platform Admins can manage Entra ID users and groups in the platform.
✓	X	✓	<ul style="list-style-type: none"> - Registration app created - Federation provider not created - Directory service created - Entra ID users cannot log on to the platform - Platform Admins can manage Entra ID users and groups in the platform.

What is the scope of the API permission "Entra ID - Read"?

Granting this permission provides READ access to users and groups across the associated Azure tenant.

Will we eventually have the same browsing experience for AD and Entra ID?

When browsing Entra ID groups and selecting an Entra ID directory, paginated results are automatically displayed making it easier to navigate and find information. However, Active Directory (AD) results are returned only after entering a search term.

How long does the Platform take to detect and reflect changes from Entra ID?

You can expect changes in Microsoft Entra ID directory objects, such as users and groups, to be updated on the Delinea platform within 10 minutes. This includes the deletion of Entra ID users and groups.

How do user attributes (e.g. mobile number) propagate from Entra ID to Platform?

User attributes supported by the Delinea Platform are automatically propagated from Entra ID, eliminating the need to configure user attribute mapping within the federation provider on the platform.

What are the advantages of configuring the Entra ID integration using the Delinea-managed registered app?

Eliminates the need to manually configure the Azure app registration and the Delinea registered app on the Delinea Platform. The Delinea Platform automatically creates the required Azure enterprise application and app registrations and manages its certificates, secrets, token settings, and API permissions.

Where is the registered app I created as part of the private preview?

The Public Preview introduced the concept of Delinea-managed apps. If a registered app was created during the Private Preview, it is now located in the Registered apps > Customer managed tab.

How are secrets managed using the Delinea-managed app?

Secrets are managed by the Delinea platform and are automatically rotated every 180 days.

How can I resolve Delinea-managed app consent errors?

If there is a consent error, check that the Microsoft account has either the Global Administrator or Privileged Role Administrator role and try to grant consent again.

Can I delete a Delinea-managed app?

Yes. Select the Delinea-managed app, right-click, and select **Delete**. This action will remove the app from the Delinea platform and delete the associated Azure app registrations, effectively removing the integration. The Azure enterprise application, *Delinea Platform Azure Registered Apps* will remain, but may be manually deleted by:

1. Navigating to Enterprise Applications in Azure
2. Selecting Delinea Platform Azure Registered Apps
3. Viewing its properties and selecting Delete

Webhooks



Note: Ensure that you have permission to view webhooks on the Delinea Platform. The permission name is *view Webhooks*.

Webhooks enable communication from the Delinea Platform to a predefined external URL. Webhooks can be used to automate tasks, send data to ITSM solutions, or integrate with other security products such as SIEM and SOAR

Webhooks

solutions. You can also use webhooks to send real-time notifications for all events created based on all services and levels.

Webhook content is structured in JSON format. You can process the .json file.

For related content, see the following:

- [Webhooks Management](#)
- [Integrating Microsoft Sentinel](#)
- [Integrating Splunk Cloud](#)
- [Integrating Splunk Enterprise](#)

Managing Webhooks

Prerequisites

Ensure that you have permission on the Delinea Platform to manage webhooks:

- **Permission name:** Manage Webhooks
- **Permission string:** delinea.platform/webhooks/manage

For more information about permissions, see the [Platform Permissions](#) table.

Creating a Webhook

1. Navigate to **Settings > General settings > Webhooks**. The Webhooks page opens.
2. Select **Create Webhook**.

The Create Webhook page opens.

Webhooks

Create Webhook

Name

Endpoint URL

Description

Webhook State ☒ Enabled

Triggers

Subscribing your webhook to specific events allows you to receive notifications only for those events you are interested in

Service

Level

Event Type

Target

Custom Headers

Optional HTTP headers for additional request configuration. By default we add token to ensure that the webhook request is legitimate

1 item

KEY	VALUE	
<input type="text"/>	<input type="text"/>	Remove

[Add Header](#)

3. On the Create Webhook page, complete the following fields:

- **Name:** Enter a unique name for the webhook to help identify it in your system.
- **Endpoint URL:** Enter a unique name for the webhook to help identify it in your system.
- **Description:** Enter a brief description of the webhook to provide context about its specific function.
- **Webhook State:** Use the checkbox to enable or disable the webhook, where checking it makes the webhook active and unchecking it disables notifications.

Triggers section

Define the events that will trigger the webhook by selecting options for service, severity level, event type, and target.

- **Service:** Select the specific service to subscribe to webhook notifications from, helping target relevant service events.
- **Level:** Choose the severity or level of events (e.g., error, warning, info) to determine which events trigger the webhook.
- **Event Type:** Select the type of event that should trigger the webhook, allowing granular control over which events cause notifications.
- **Target:** Add a specific target for the webhook notifications to filter and direct them to the correct recipient or system.

Custom Headers section

Define additional HTTP headers (e.g., Authorization, API-Key) to be included in the webhook requests, enabling customization of the HTTP request headers.

Webhooks

- **Key:** Enter the name of the custom header to specify its type (e.g., Authorization, API-Key) for the webhook request.
Note: Use the Add Header hyperlinked button if you want to add more custom headers to the webhook request to allow for additional configuration options.
- **Value:** Enter the corresponding value for the custom header to ensure the correct data is included in the webhook request.
Note: Use the Remove hyperlinked button to remove a specific header entry when it's no longer needed or accurate for the webhook configuration.

When you are finished completing the fields on the Create Webhook page, select **Save** to create your webhook with your specified configurations.

Managing Webhooks

To access available webhooks or to create a new one, navigate to **Settings > Webhooks**.

The screenshot displays the 'Webhooks' management interface. On the left, a sidebar contains a navigation menu with 'Settings' highlighted. The main panel shows the 'Webhooks' tab, which includes a search bar and a table of 6 items. The table columns are NAME, TRIGGERS, ENDPOINT URL, STATE, and LAST RUN STATUS. The items listed are 'checks test', 'all itp', 'test', 'demo splunk', 'my test', and 'shir test'. The 'checks test' item has a 'Failed' status, while the others are 'Success' or 'Failed'.

NAME	TRIGGERS	ENDPOINT URL	STATE	LAST RUN STATUS
checks test	All services / All event levels	https://webhook.site/9ccod...	Enabled	Failed
all itp	ITP / System Activity	https://webhook.site/4f62f0...	Enabled	Success
test	ITP / System Activity / Check Failed, Incident ...	https://webhook.site/d7f288...	Enabled	Failed
demo splunk	Permission / Security Audit	https://prd-p-6wjc0.splunkcl...	Enabled	Failed
my test	All services / All event levels	https://webhook.site/a3c418...	Enabled	Failed
shir test	All services / All event levels	https://webhook.site/5c029...	Enabled	Failed

On the Webhooks page, two tabs are available: **Webhooks** and **Logs**:

Webhooks

- **Webhooks:** On the Webhooks tab, you can see all available webhooks. The following columns are displayed:

- **Name:** The name of the webhook.
- **Triggers:** The specific platform events or actions that trigger the webhook, such as user logins, secret access, or policy changes.
- **Endpoint URL:** The URL to which the webhook sends event data. This is the endpoint specified when configuring the webhook where platform events are delivered.
- **Created By:** The user who created the webhook. This is especially useful in team or multi-user environments.
- **Created At:** The timestamp indicating when the webhook was initially created.
- **State:** The state of the webhook, for example **Enabled** (active) or **Disabled** (inactive).
- **Last Run Status:** The status of the most recent webhook execution, for example "Success," "Failed," "Pending").

- **Logs:** On the Logs tab, the following columns are displayed:

- **Name:** The name or identifier of the webhook event or configuration.
- **Status:** The status of the webhook, for example Success, Failure.
- **Triggers:** The specific events or actions that you choose to be notified about.
- **Created By:** The user or account that created the webhook configuration.
- **Sent At:** The timestamp indicating when the webhook event was sent to the specified endpoint.



Note: On both tabs, you can use the grid button to choose only the columns you wish to see.

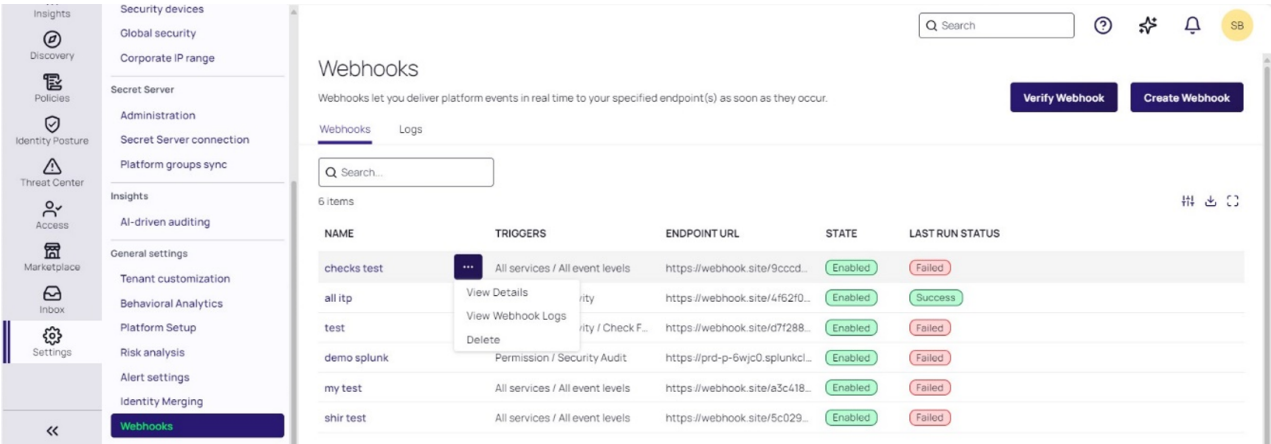
The screenshot shows the 'Webhooks' tab in a software interface. At the top, there's a header 'Webhooks' with a description: 'Webhooks let you deliver platform events in real time to your specified endpoint(s) as soon as they occur.' Below this are two buttons: 'Verify Webhook' and 'Create Webhook'. A tab bar shows 'Webhooks' and 'Logs'. A search bar is present. Below the search bar, it says '763 items'. A table displays a list of webhooks with columns: NAME, STATUS, TRIGGERS, and SENT AT. The STATUS column shows '404-Fail' for all entries. A 'Displayed columns' dialog box is open on the right, showing a list of columns with checkboxes: Name (checked), Status (checked), Triggers (checked), Created By (unchecked), and Sent At (checked). The dialog has 'Cancel' and 'Save' buttons.

NAME	STATUS	TRIGGERS	SENT AT
checks test	404-Fail	Identity / Security Audit / Delinea.Identity.AuthSess...	12/19/24, 10:46 AM
checks test	404-Fail	Secret Server / Privileged Activity / Delinea.Vault.Se...	12/19/24, 10:43 AM
checks test	404-Fail	Secret Server / Privileged Activity / Delinea.Vault.Se...	12/19/24, 10:43 AM
checks test	404-Fail	Secret Server / Privileged Activity / Delinea.Vault.Se...	12/19/24, 10:34 AM
checks test	404-Fail	Secret Server / Privileged Activity / Delinea.Vault.Se...	12/19/24, 10:33 AM
checks test	404-Fail	All services / All event levels / Webhook Testing	12/19/24, 10:31 AM
checks test	404-Fail	Identity / Privileged Activity / Delinea.Cloud.Core.M...	12/19/24, 10:24 AM

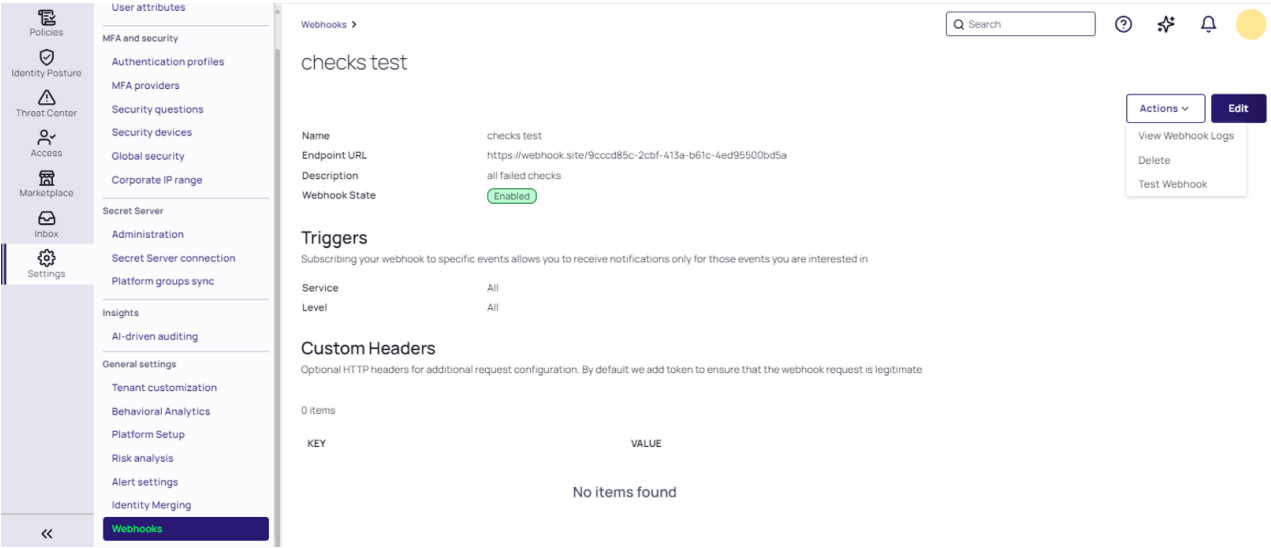
To manage your webhooks:

Webhooks

1. Navigate to **Settings > General settings > Webhooks**. The Webhooks page opens.



2. Select your webhook from the list.
3. Select **Edit** to change the configurations for the webhook.
4. Select the **Actions** drop-down menu.



From the Actions dropdown you can select:

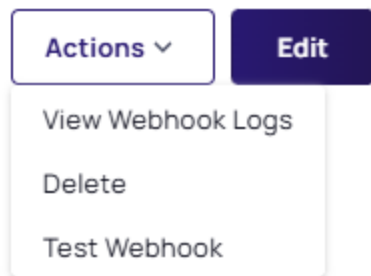
- **Delete** to delete the selected webhook
- **Test Webhook** to test the created webhook
- **View Webhook Logs** to display the webhook logs.

Webhook Logs

There are three ways to view the webhook logs from the Webhooks page:

Webhooks

- Select the **Logs** tab, or...
- Select a webhook to open it, click the **Actions** drop-down menu, and choose **View Webhook Logs**, or...



- Hover over the webhook row, click the ellipses (...) that appears, and select the **View Webhook Logs** option.

Webhooks

Webhooks let you deliver platform events in real time to your specified endpoint(s) as soon as they occur.

Webhooks Logs

Q Search...

6 items

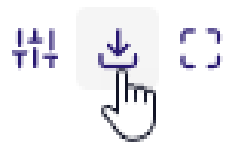
NAME	TRIGGERS	ENDPOINT URL
checks test	⋮ All services / All event levels	https://webhook
all itp	View Details /ity	https://webhook
test	View Webhook Logs /ity / Check Failed, Incident Created	https://webhook
demo splunk	Delete Permission / Security Audit	https://prd-p-6i

Here you can also delete the webhook by selecting the **Delete** option, or see details by selecting the **View Details** option.

To download webhook logs:

Webhooks

1. Select the Download icon.



The Download page opens.

Download

Download CSV

Records 390

File name

Date format

ISO (2024-12-19T08:47:34.006Z)	▼
ISO (2024-12-19T08:47:34.006Z)	✓
User format (12/19/24, 10:47 AM)	

2. On the Download page, specify the logs to download using the fields presented:

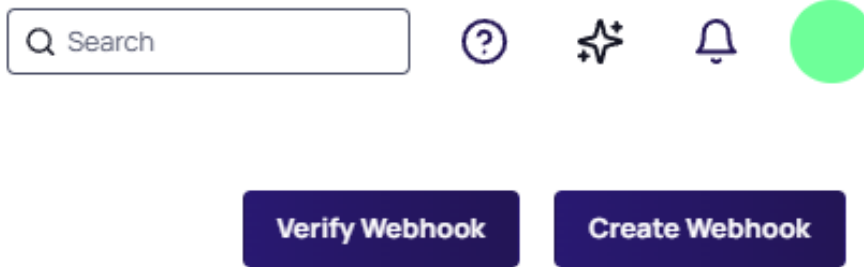
- **Records:** Specify the number of records to include in the logs.
- **File Name:** Enter a name for the webhook log file to make it easier to locate.
- **Date Format:** Select your preferred date format from the drop-down menu.

Verifying a Webhook

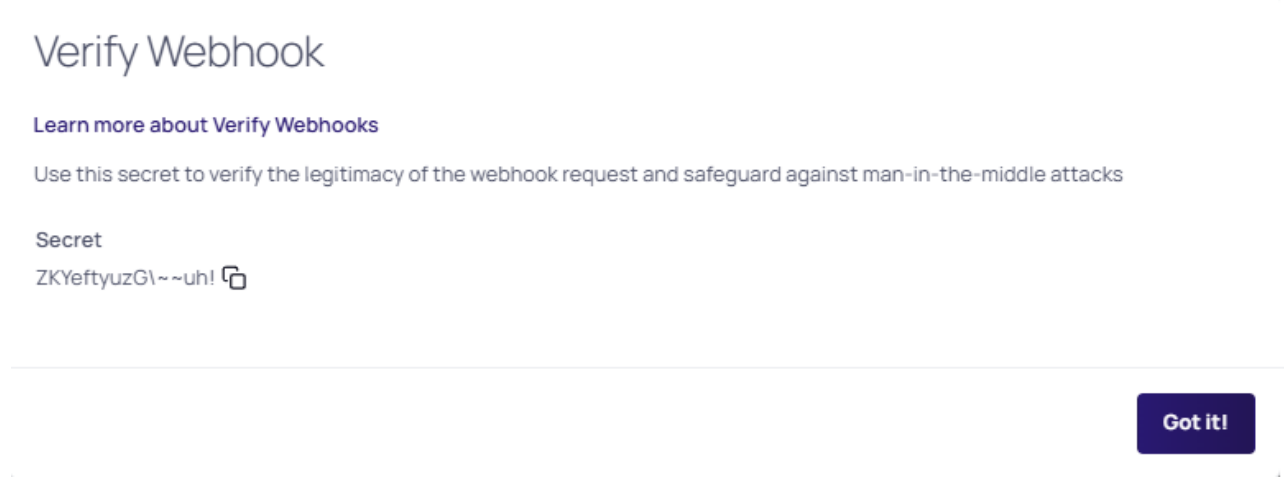
Complete the following steps to validate the incoming webhook payloads against the token and verify that they are from Delinea and have not been tampered with:

Webhooks

1. Navigate to **Settings > General settings > Webhooks**. The Webhooks page opens.
2. Select **Verify Webhook**.



The Verify Webhook page opens.



3. On the Verify Webhook page, copy the secret token and store it in a secure and accessible server location. Delinea will use your secret token to create a hash signature that is sent to you with each payload. The hash signature will appear in each delivery as the value of the X-Token header.
4. Select **Got it!** to close the page.

Calculating Hash

In your code that handles webhook deliveries, calculate a hash using your secret token. Then compare the hash sent by Delinea with the expected hash you calculated to ensure that they match.

Python Example

You can use the following `verify_signature` function and call it when you receive a webhook payload:

Python Example

```
import base64

import hashlib
```

Webhooks

```
import hmac

import json

def verify_signature(payload_body: dict, secret_token: str, signature_header: str):
    """Verify that the payload was sent from Delinea by validating SHA256.

    Raise and return 403 if not authorized.

    Args:
        payload_body: original request body to verify (request.body())
        secret_token: Delinea app webhook token (WEBHOOK_SECRET)
        signature_header: header received from Delinea(x-hub-signature-256)
    """
    if not signature_header:
        raise HTTPException(status_code=403, detail="x-signature header is missing!")

    payload = json.dumps(payload_body).encode("utf-8")

    signature = base64.b64decode(signature_header)

    digest = hmac.new(secret_token.encode("utf-8"), msg=payload,
        digestmod=hashlib.sha256).digest()

    if not hmac.compare_digest(digest, signature):
        raise HTTPException(status_code=403, detail="Request signatures didn't match!")
```

Integrating Microsoft Sentinel

Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution for proactive threat detection, investigation, and response. You can integrate Microsoft Sentinel with the Delinea Platform by using webhooks.

Prerequisites

Ensure that you have all the required accounts and utilities before starting the integration:

- Admin account on the Delinea Platform
- Azure subscription

Webhooks

- Access to the Microsoft Sentinel portal
- Log Analytics workspace

Important: This integration does not rely on the deprecated Log Analytics Agent, which was retired on August 31, 2024. Instead, it leverages HTTP requests to trigger Azure Logic Apps workflows that generate custom log entries or alerts in Azure Sentinel. This integration does not depend on either the Log Analytics Agent or the Azure Monitor Agent (AMA), ensuring a modern, agentless solution.

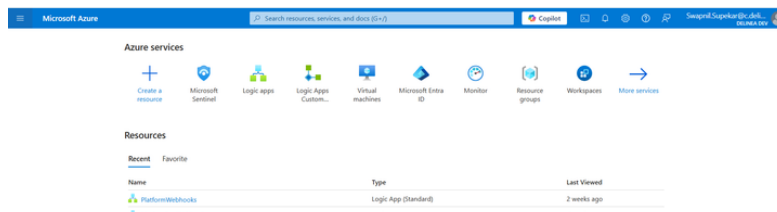
Configuring Microsoft Sentinel

To configure Microsoft Azure Sentinel, create a Logic app and set up Sentinel Log Analytics.

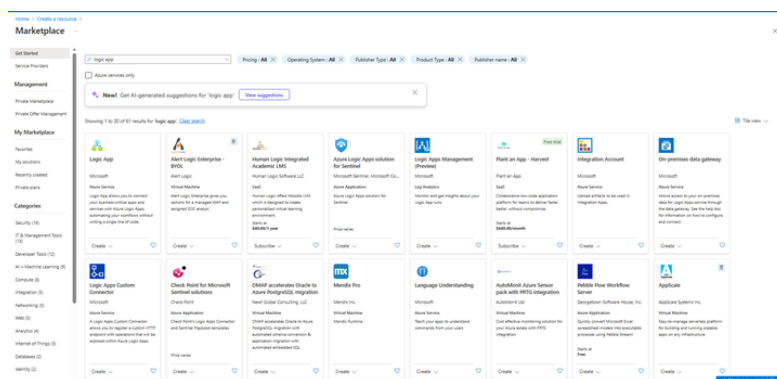
Creating a Logic App in Sentinel

To create a logic app:

1. Log in to the Azure portal dashboard.
2. In the services section, select **Create a resource**.



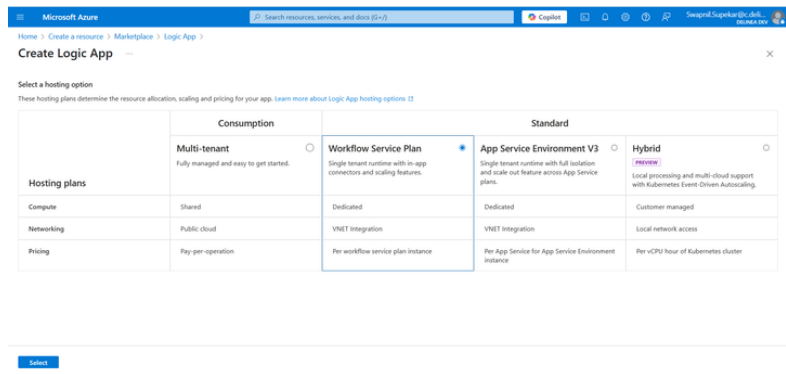
3. Enter *Logic App* in the search area, and then select **Logic App**.



4. Select **Create**.

Webhooks

5. Select the **Workflow Service Plan** check box.

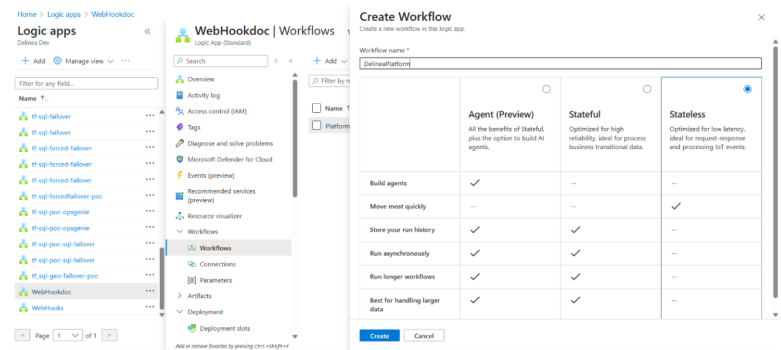


6. Click **Select**.
7. Fill in the required information for your Logic App and select **Review + Create**.
8. Once the deployment is done, your Logic App is created in Sentinel.

Setting up Sentinel Log Analytics

To set up Sentinel log analytics:

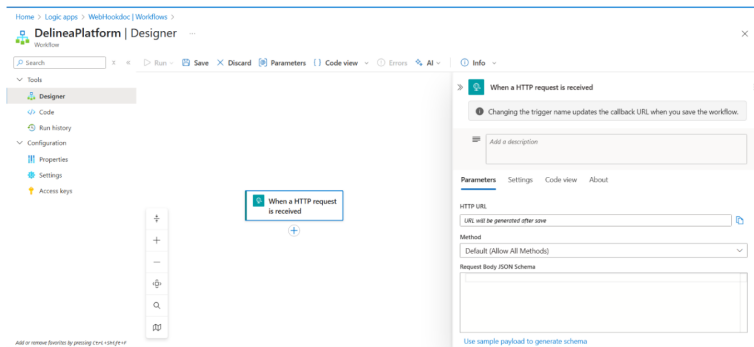
1. In the Logic App, go to **Workflows** and select **Add** to add a new workflow. The *Create Workflow* window opens.
2. Enter the **Workflow Name** and select **Stateless** as the state type.



3. Select **Create**. Note: Depending on screen resolution, the **Create** button might be hidden at the bottom of the app tile.
4. Open the newly-created workflow.

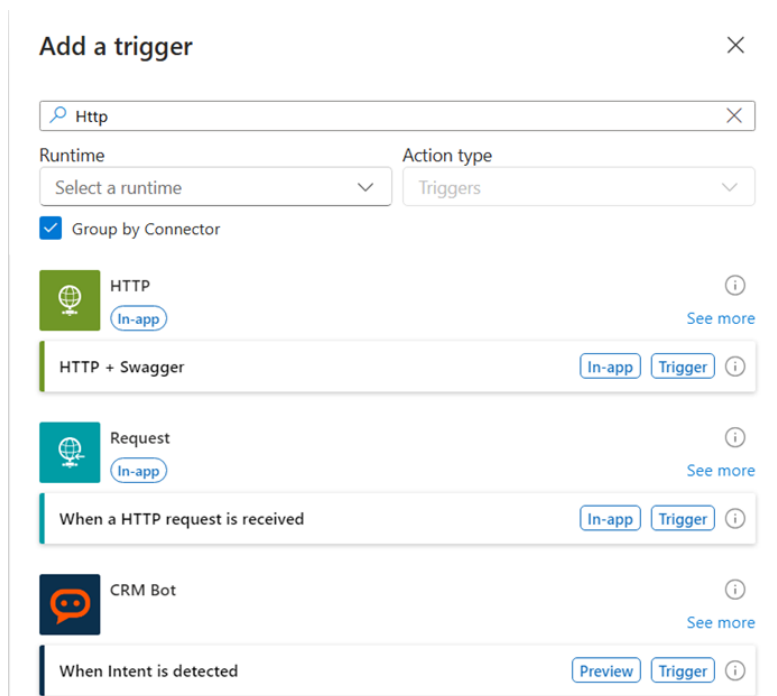
Webhooks

5. Navigate to **Tools > Designer**.



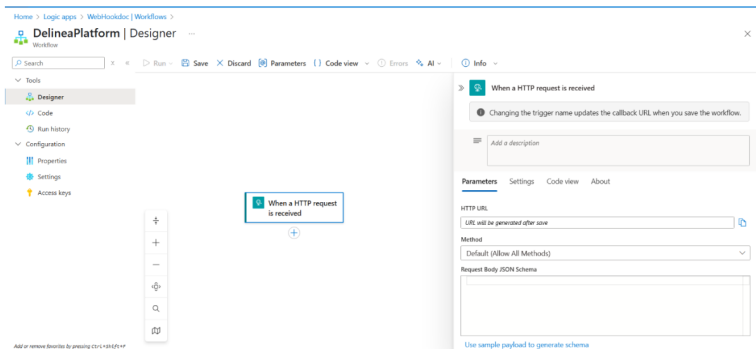
6. On the *Designer* page, select the plus sign, then select **Add trigger**.

7. Search for "HTTP" and select **When an HTTP request is received** in the Request section. You will use this trigger later when setting up a webhook on the Delinea Platform.



Webhooks

8. Select the **Use sample payload to generate schema** hyperlink.



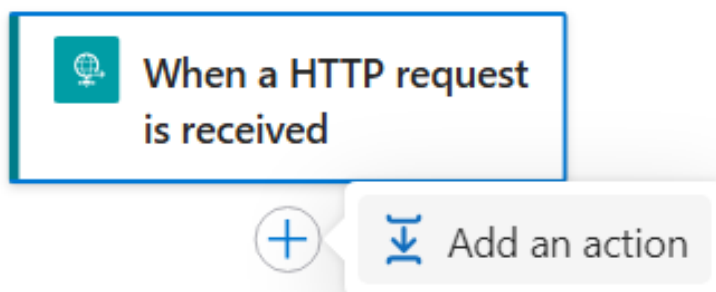
9. Paste the following code into the field. (Alternatively, you can retrieve the schema payload from the **Marketplace >Test webhook Request body**) :

```
{  
  "AuditEventMessageId": "87b928df-ccc5-46ed-8cc5-b2e88866a2b5",  
  "TenantId": "7968fc7c-9205-4bd8-ad41-1432ffb8f7d3",  
  ...  
  "ForceCompress": false  
}
```

10.

11. Select **Done**, then select **Save**.

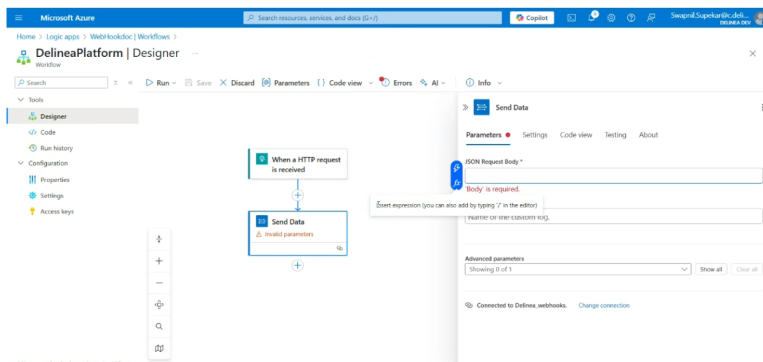
12. Select the plus sign and then select **Add an action**.



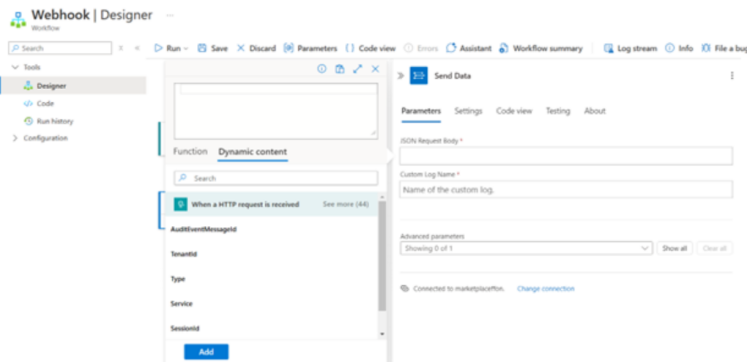
13. Search for "Log Analytics" and select **Send Data**. The *Create a connection* page opens.
14. Provide the **Workspace ID** and **Shared Key**. Where to Find Your Workspace ID and Key:

Webhooks

- a. In the Sentinel portal, go to **Home > Microsoft Sentinel**.
 - b. Navigate to **Settings > Workspace settings > Settings > Agents**.
 - c. Click the arrow icon to expand the **Log Analytics agent instructions**.
15. Copy your **Workspace ID** and either the **Primary Key** or **Secondary Key**.
 16. Paste the Workspace ID into the Create new connection page.
 17. Select **Create New**.
 18. The Send Data page opens. Under the Parameters tab, select the **JSON Request Body** field, and select the second option.

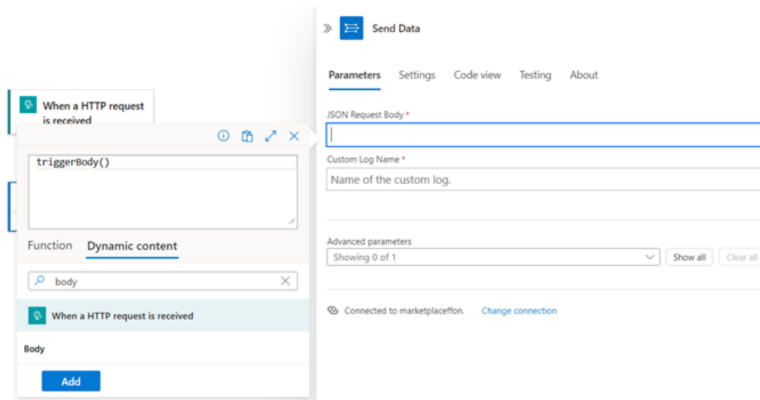


19. Select the **Dynamic content** tab and enter 'Body' in the Search field.

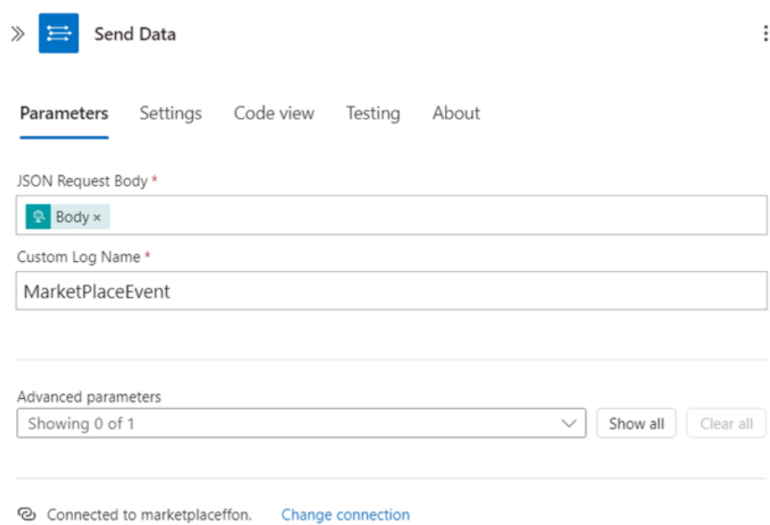


Webhooks

20. Select the body then select **Add**.



21. Provide a new name for the Custom Log Name (e.g. MarketPlace Event)



22. Select **Save**.

Integrating Webhooks and Microsoft Sentinel

To integrate webhooks and Microsoft Sentinel, follow these steps.

1. Log in to the Delinea Platform.
2. From the left navigation menu, select **Settings**, then **Webhooks**.

Webhooks

3. On the Webhooks page, click **Create Webhook**.

Webhooks

Webhooks let you deliver platform events in real time to your specified endpoint(s) as soon as they occur.

Verify Webhook

Create Webhook

Webhooks

Logs

Q Search...

6 items

NAME	TRIGGERS	ENDPOINT URL	STATE	LAST RUN STATUS
checks test	All services / All event levels	https://webhook.site/9cccd85c-2cbf-413a-b61c-4ed95500bd5a	Enabled	Failed
all itp	ITP / System Activity	https://webhook.site/4f62f02c-9164-4661-be7a-65af52537b30	Enabled	Success
test	ITP / System Activity / Check Failed, Incident Created	https://webhook.site/d72887f-26df-42b9-86c0-932c12993a5d	Enabled	Failed
demo splunk	Permission / Security Audit	https://prd-p-6wj0.splunkcloud.com:8088/services/collector/raw	Enabled	Failed
my test	All services / All event levels	https://webhook.site/a3c41899-6ce9-4ebd-b019-0c0491b24987	Enabled	Failed
shir test	All services / All event levels	https://webhook.site/5c029627-6880-4a83-8845-ef53492223c3	Enabled	Failed

4. In the **Endpoint URL** field, enter the HTTP request URL—an HTTP trigger configured in the Logic App.

Create Webhook

Name

Endpoint URL

Description

Webhook State

☒ Enabled

Triggers

Subscribing your webhook to specific events allows you to receive notifications only for those events you are interested in

Service

All ▾

Level

All ▾

Event Type

All ▾

Target

Add

Custom Headers

Optional HTTP headers for additional request configuration. By default we add token to ensure that the webhook request is legitimate

1 item

KEY

VALUE

Remove

Add Header

Cancel

Save

5. Select **Save**.
6. Verify the configured webhook on the Delinea Platform (see [Testing a webhook](#)).

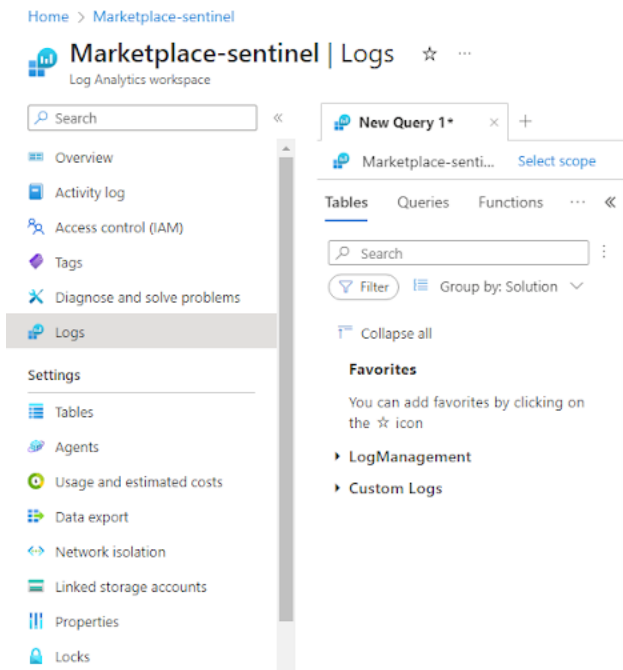
Verifying Logs for the Microsoft Sentinel Webhook

After you have set up the integration, we recommend verifying that the Delinea Platform events are being collected for Azure Sentinel.

1. Log in to the Delinea Platform and perform an activity that will generate a new audit log.
2. Open your Logic App.

Webhooks

3. Select the activity log and verify that logs from the Delinea Platform are triggered automatically.
4. Go to the Sentinel dashboard in the Microsoft Sentinel Portal.
5. From the left navigation menu, select **Logs**.



6. In the query editor, enter the following KQL query:

```
MarketPlaceEvents_CL  
| order by TimeGenerated desc  
| take 10
```

7. Verify that the log is displayed.

The screenshot shows the KQL query results in the Microsoft Sentinel interface. The query editor at the top contains the query: `MarketPlaceEvents_CL | order by TimeGenerated desc | take 10`. Below the editor, the 'Results' tab is active, displaying a table with 10 rows of log data. The table has columns for TimeGenerated, AdditionalAttributes, and TargetHost. The data shows events from the Delinea.Auditing.Shared EventSource, System.Collections.Generic.

TimeGenerated [UTC]	AdditionalAttributes_ADD_S...	AdditionalAttributes_SS...	AdditionalAttributes_SS...	AdditionalAttributes_SS...	AdditionalAttributes_SS...	AdditionalAttributes_SS...	TargetHost_type_s	Tags_type_s
3/13/2023, 6:00:12:188 AM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/13/2023, 6:00:12:149 AM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 7:57:40:590 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 7:57:38:395 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 7:13:50:165 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 7:12:51:725 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 7:12:01:523 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 6:02:57:474 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 6:02:57:474 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...
3/12/2023, 5:53:56:714 PM	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	[{"03/28/2023 00:00:00P6/30/2...	Delinea.Auditing.Shared EventA...	System.Collections Gener...

Integrating Splunk Enterprise

Splunk Enterprise technology analyzes business and website data, manages applications, ensures compliance, and enhances security.

You can integrate Splunk Enterprise with the Delinea Platform using webhooks.

Prerequisites

Ensure that you have all the required accounts and utilities before starting the integration:

- Account on the Delinea Platform
- Account in [Splunk Enterprise](#)
- Installed [OpenSSL](#) on local computer
- Installed [Docker container for Splunk Enterprise](#)

Setting Up Splunk Enterprise

To configure Splunk Enterprise, create an SSL certificate and generate a private key with the appropriate files to combine your SSL/TLS certificate, intermediate certificates (if applicable), and the private key into a single file.

Creating a Certificate in Zero SSL

You can create an SSL certificate from any certificate provider. The instructions below are for creating an SSL certificate issued by Zero SSL.

1. Go to [Zero SSL](#).
2. Open the **SSL Certificates** panel.
3. Click **New Certificate**.
4. Provide a valid domain for the certificate, then click **Next Step** until the Verify Domain dialog appears.

New Certificate Cancel

SSL Certificate Setup

You're on your way to issuing a brand-new SSL certificate for one or multiple domains. Before you can install your new certificate, please complete the steps below.

☒ Domains

☐ I need a wildcard certificate PRO

Please enter at least one domain to secure. For single-domain certificates the WWW-version of your domain will always be included at no extra charge.

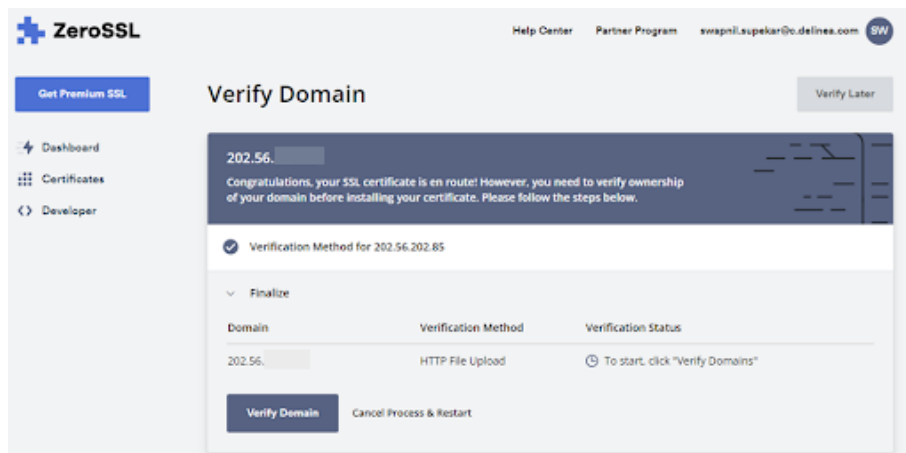
Enter Domains

<input type="text" value="202.56.202"/>	<input checked="" type="checkbox"/> 202.56.202
---	--

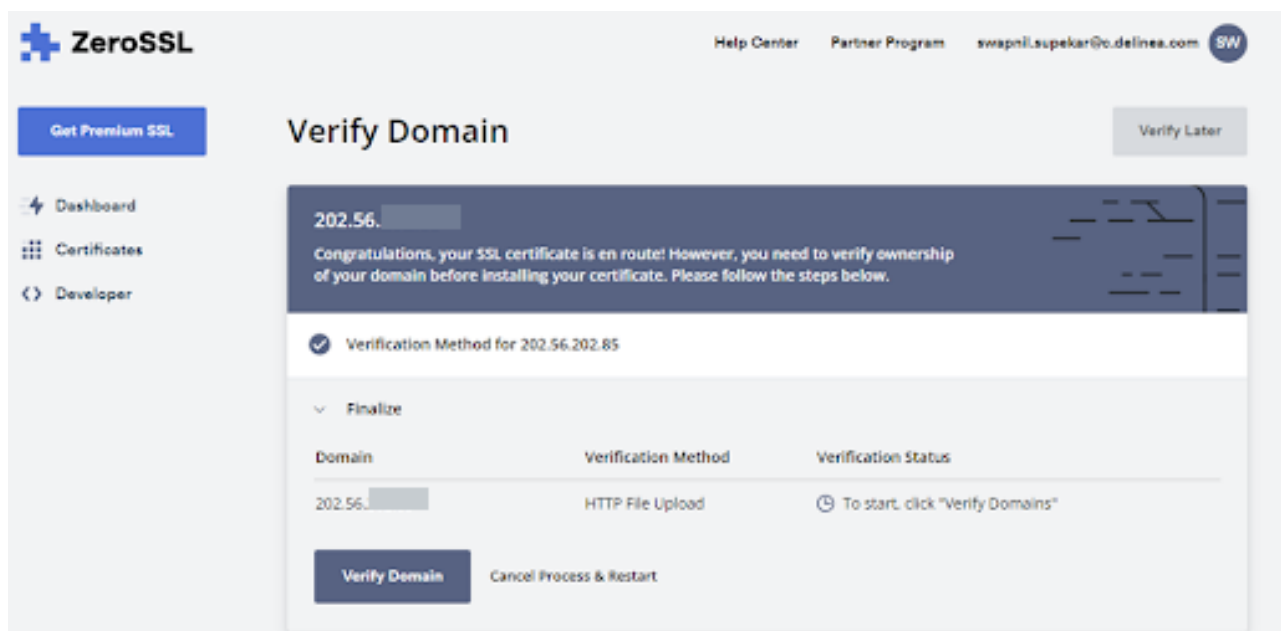
PRO →

Webhooks

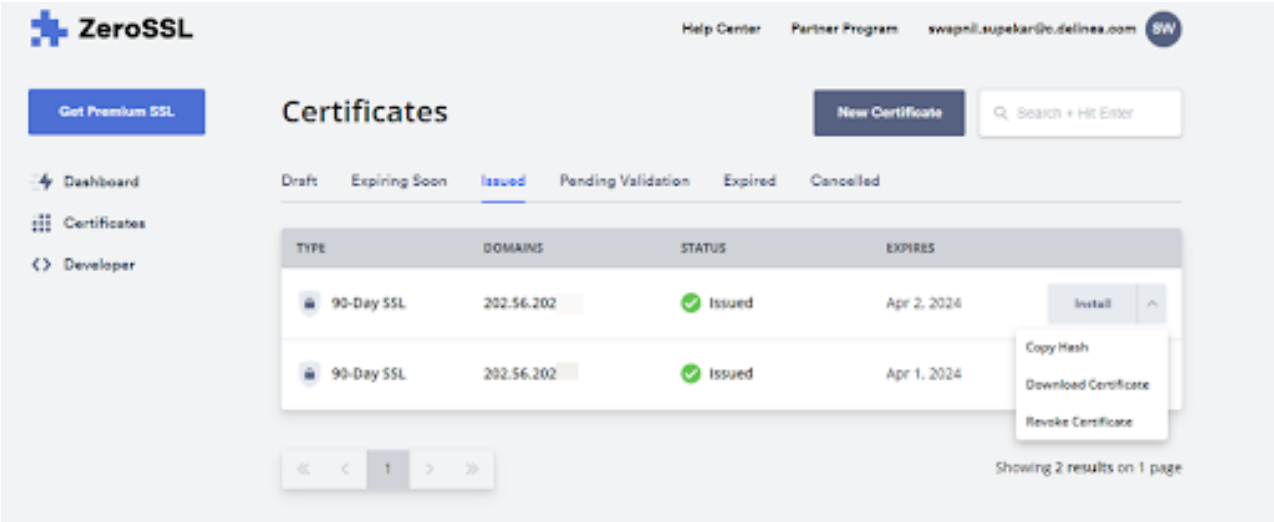
5. In the **Verify Domain** dialog, select an **HTTP File Upload** and follow the instructions.



6. Select **Next Step**.
7. In the Verify Domain dialog, check the details for the certificate verification and click **Verify Domain**.



8. Once done, go to the **Certificates** panel, select your certificate, and download it.



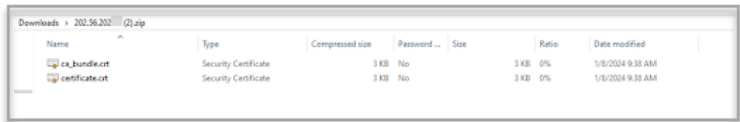
Configuring a Certificate in OpenSSL

To configure a certificate in OpenSSL, generate private key (`private.pem`), `caCertificateFile` (`certificate.pem`), and full chain (`full_chain.pem`) files.

Generating a Private Key

To generate a private key file in OpenSSL:

1. Copy the downloaded certificate to the Splunk directory on your local computer. For example:
`c:/programfiles/splunk/etc/auth/sloccerts`



2. Verify that you have **OpenSSL** installed on your computer.
3. Depending on your operating system, open a terminal or a command prompt.
4. Navigate to the directory where you want to generate a private key. You can use the `cd` command to change directories.

```
bash
cd path/to/your/directory
```

5. Run the following command to generate a private key:
`openssl genpkey -algorithm RSA - out private.key`

The command generates a private key using the RSA algorithm and saves it to a private key file. You can adjust the algorithm or key size according to your preferences.

Generating a caCertificateFile

To generate a caCertificateFile, create a Certificate Signing Request (CSR) and then self-sign it. Open a terminal or a command prompt and run the following commands:

1. To generate a Certificate Signing Request (CSR):

```
openssl req -new -key ca_private_key.pem -out ca_csr.pem
```

This command generates a Certificate Signing Request (CSR) using the private key ca_private_key.pem and saves it to ca_csr.pem.

2. To self-sign a Certificate Signing Request (CSR):

```
openssl x509 -req -days 365 -in ca_csr.pem -signkey ca_private_key.pem -out ca_certificate.pem
```

Generating a full_chain.pem file

A full_chain.pem file typically combines your SSL/TLS certificate, intermediate certificates (if applicable), and the private key into a single file. The order of the certificates is crucial for proper functioning.

Assuming you have the following components:

- Your SSL/TLS certificate (for example, your_certificate.crt)
- Intermediate certificate(s) (if provided by your Certificate Authority)
- Your private key (for example, a private.key)

To generate a full_chain.pem file using these components:

1. Run the following command in the Splunk directory on your computer. Replace your_certificate.crt with the actual name of your SSL/TLS certificate file, replace intermediate.crt with the name of any intermediate certificate file (if applicable), and replace private.key with the name of your private key file:

```
cat your_certificate.crt intermediate.crt private.key > full_chain.pem
```

Ensure that you concatenate the files correctly: certificate, intermediate certificate(s), and finally the private key. The resulting full_chain.pem file should contain all the necessary information in the correct order.

2. After you create the full_chain.pem file, use it in your Splunk configuration for SSL/TLS settings, including configuring the sslRootCAPath parameter to point to this file.
3. Go to the Splunk directory on your local computer.
4. Open the inputs.conf file and specify the following data:

```
[http]
disabled = 0
index = main
enableSSL = 1
port = [port]
privKeyPath = $SPLUNK_HOME/etc/auth/sloccerts/private.key
serverCert = $SPLUNK_HOME/etc/auth/sloccerts/full_chain.pem
caCertFile = $SPLUNK_HOME/etc/auth/sloccerts/certificate.pem
```

Webhooks

```
sslPassword = [SSL password]  
db17Z
```

5. Open the `web.conf` file and specify the following data:

```
[settings]  
enableSplunkWebSSL = true  
httpport = [http port]  
enableSplunkWebSSLDebug = true
```

6. Restart your Splunk server.

Integrating Webhooks and Splunk Enterprise

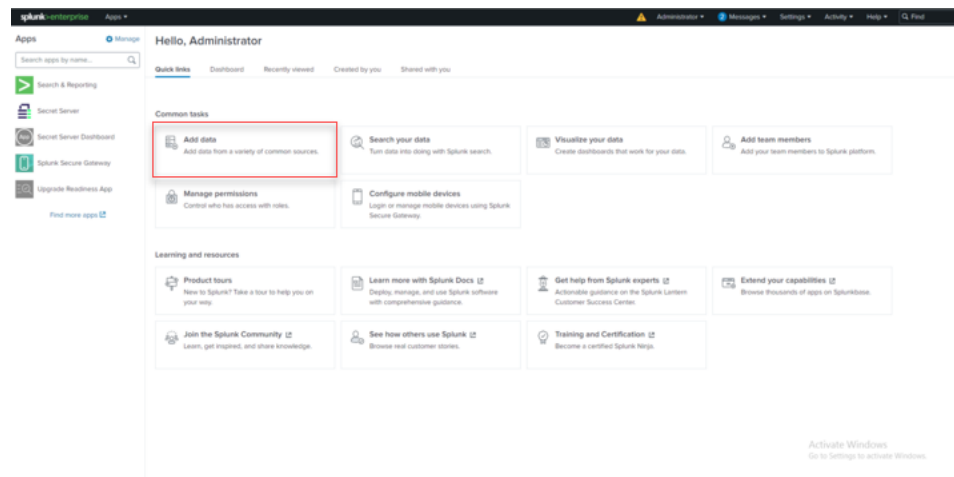
After you have generated and managed certificates, you can set up integration between Splunk Enterprise and Delinea Platform webhooks.

Configuring Splunk Enterprise HTTP Event Collector

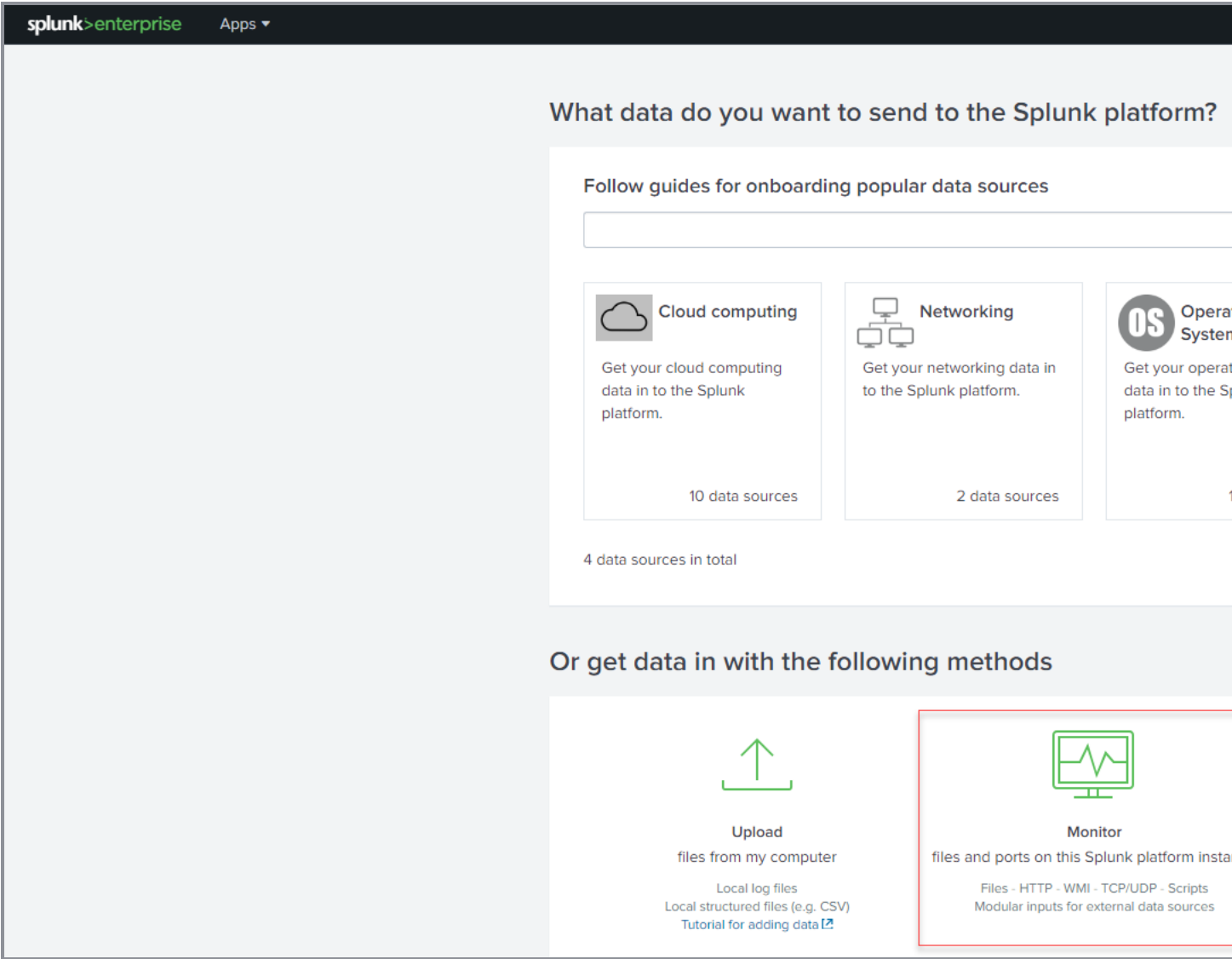
1. Install a Docker container to run Splunk Enterprise inside it. See the [Splunk Enterprise official documentation](#).
2. Open a Docker container and run Splunk Enterprise with an extra port exposed for HTTP Event Collector (HEC) using the following command:

```
docker run -d -p 8000:8000 -p 8088:8088 -e SPLUNK_START_ARGS='--accept-license' -e SPLUNK_PASSWORD=[password] splunk/splunk:latest
```

3. Log in to your Splunk Enterprise account with admin permissions.
4. On the **Quick links** tab, click **Add Data**.

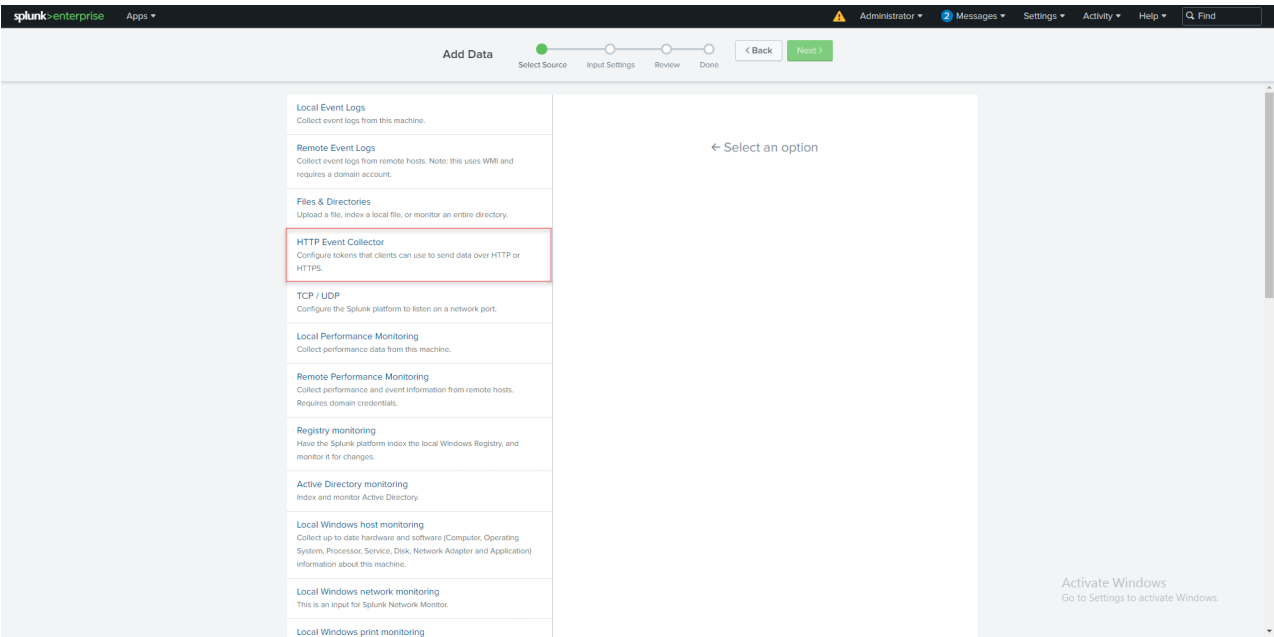


5. Select **Monitor**.

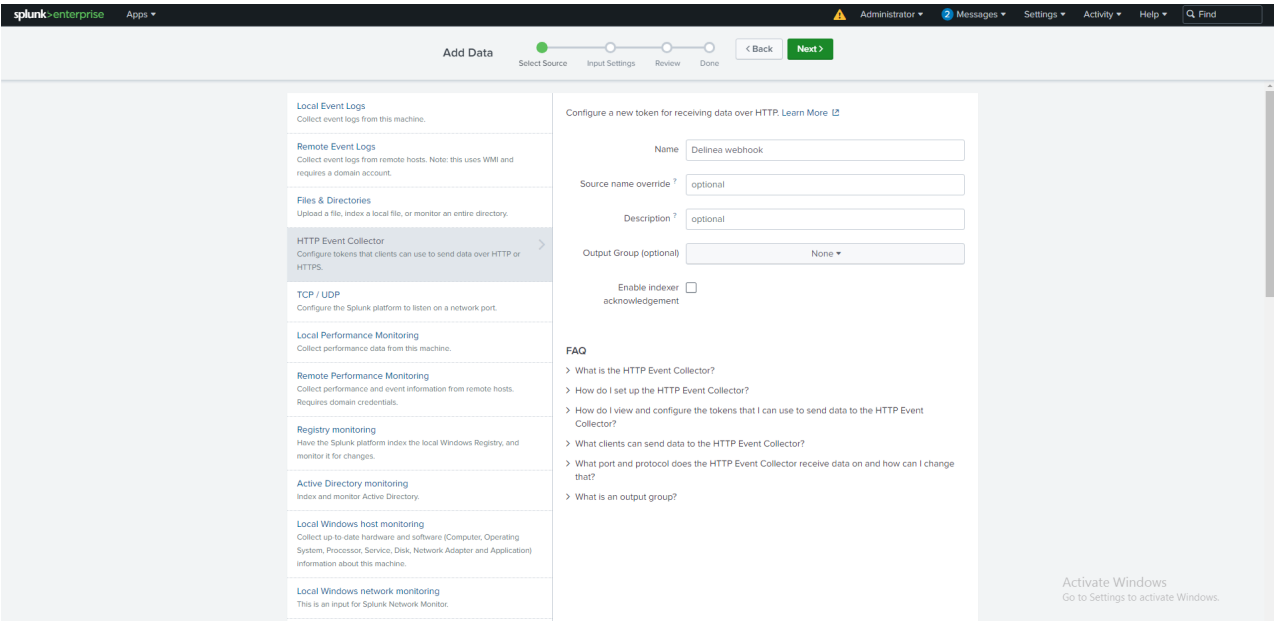


6. From the left panel, select **HTTP Event Collector**.

Webhooks

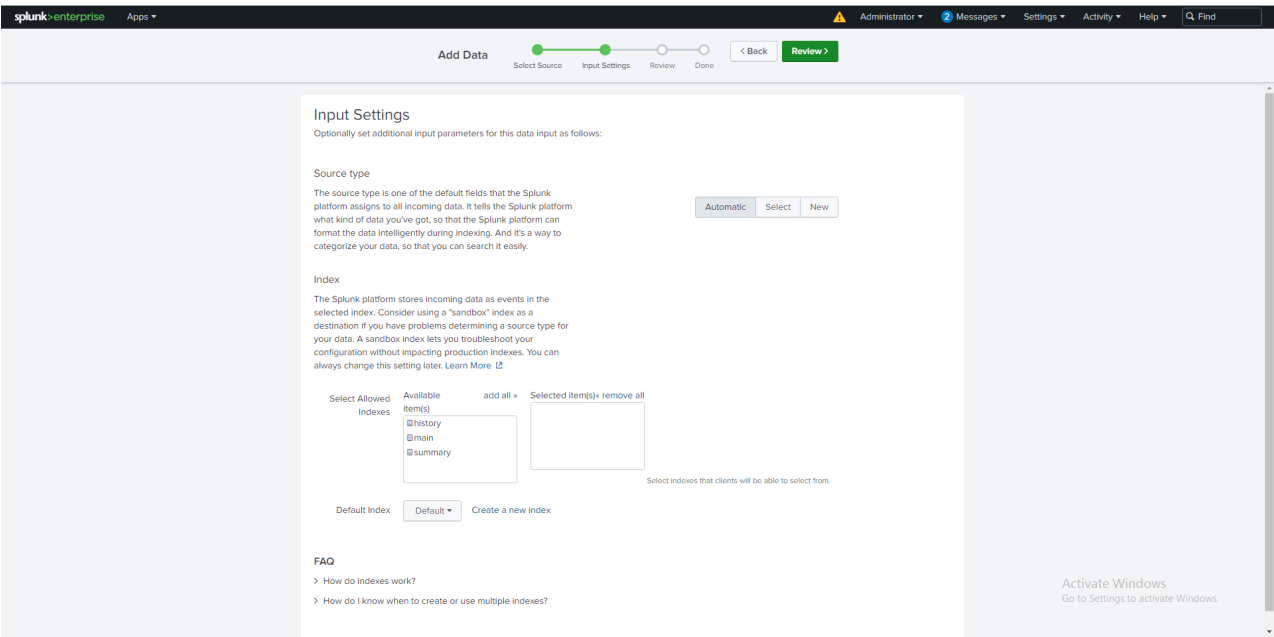


7. In the HTTP Event Connector form, specify the required details and select **Next**.

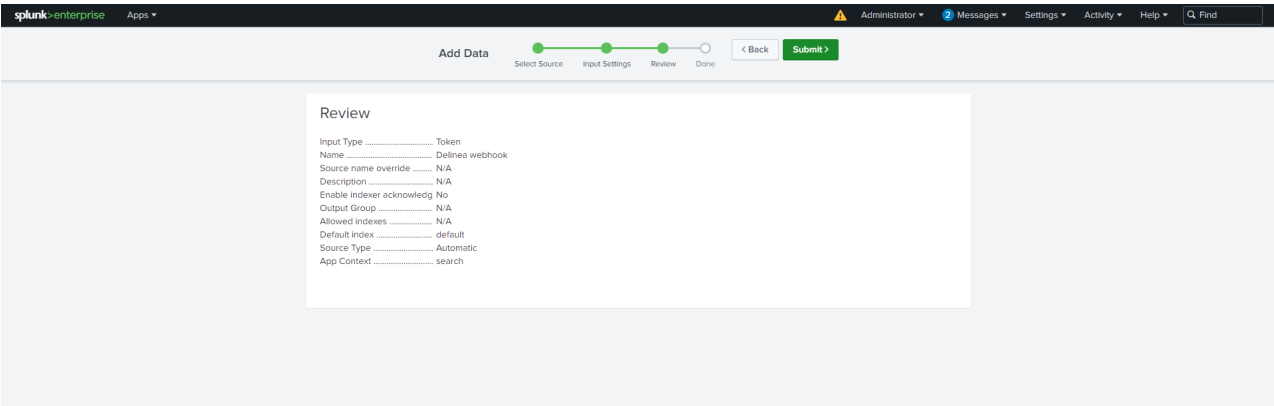


8. Check the displayed details, then select **Review**.

Webhooks

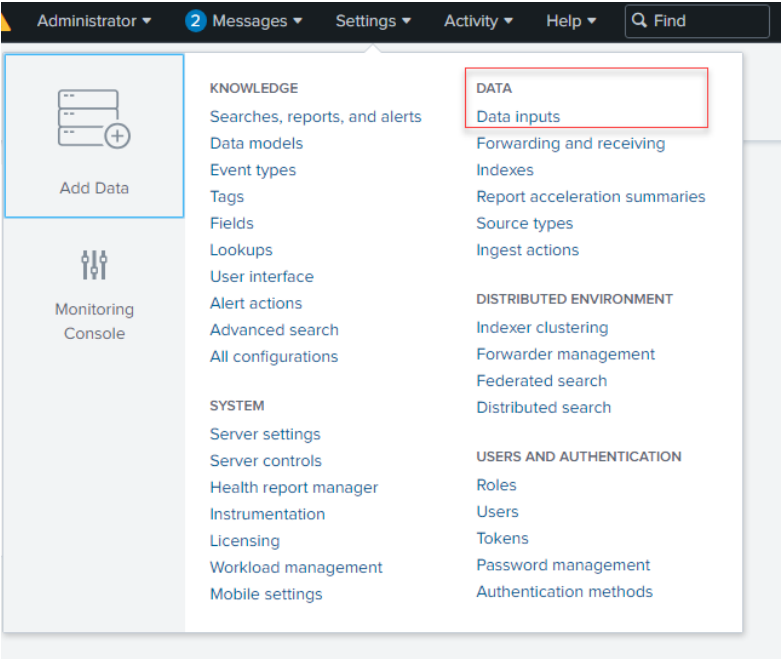


9. Select **Submit**.

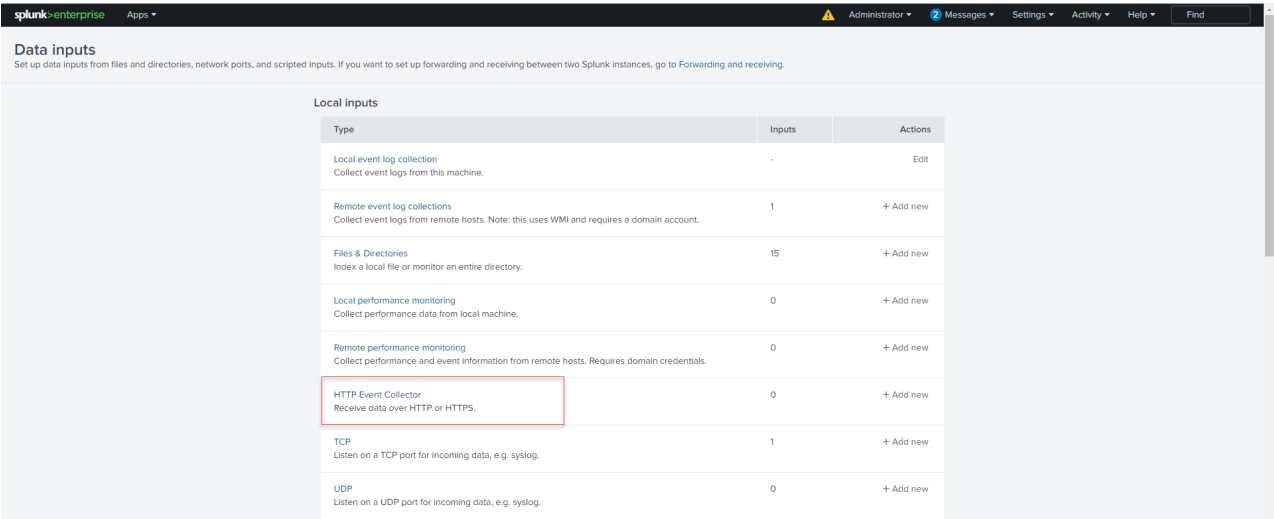


10. Go to **Settings > Add Data > Data inputs**.

Webhooks

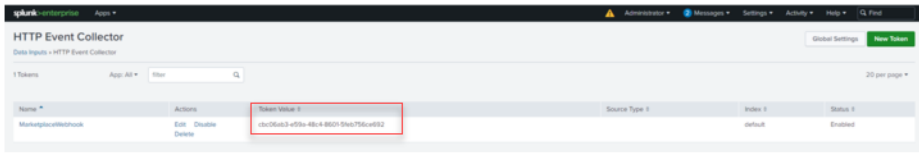


11. In the Data inputs dialog, select **HTTP Event Collector**.



12. In the HTTP Event Collector dialog, copy a **Token Value**. You will use this Token Value when creating a webhook on the Delinea Platform.

Webhooks



Creating Webhooks for Splunk Enterprise

- 1. Log in to the Delinea Platform.
- 2. From the left navigation menu, select Settings > Webhooks.
- 3. On the Webhooks page, select **Create Webhook**.

Webhooks

Webhooks let you deliver platform events in real time to your specified endpoint(s) as soon as they occur.

Verify Webhook

Create Webhook

Webhooks

Logs

Q Search...

6 items

#

↓

↺

NAME	TRIGGERS	ENDPOINT URL	STATE	LAST RUN STATUS
checks test	All services / All event levels	https://webhook.site/9cccd85c-2cbf-413a-b61c-4ed95500bd5a	Enabled	Failed
all itp	ITP / System Activity	https://webhook.site/4f62f02c-9164-4661-be7a-65af52537b30	Enabled	Success
test	ITP / System Activity / Check Failed, Incident Created	https://webhook.site/d7f2887f-26df-42b9-86c0-932c12993a5d	Enabled	Failed
demo splunk	Permission / Security Audit	https://prd-p-6wjco.splunkcloud.com:8088/services/collector/raw	Enabled	Failed
my test	All services / All event levels	https://webhook.site/a3c41899-6ce9-4ebd-b019-0c0491b24987	Enabled	Failed
shir test	All services / All event levels	https://webhook.site/5c029627-6880-4a83-8845-ef53492223c3	Enabled	Failed

The Create Webhook dialog opens.

Webhooks

Create Webhook

Name	<input type="text"/>
Endpoint URL	<input type="text"/>
Description	<input type="text"/>
Webhook State	<input checked="" type="checkbox"/> Enabled

Triggers

Subscribing your webhook to specific events allows you to receive notifications only for those events you are interested in

Service	<input type="button" value="All ▼"/>
Level	<input type="button" value="All ▼"/>
Event Type	<input type="button" value="All ▼"/>
Target	<input type="button" value="Add"/>

Custom Headers

Optional HTTP headers for additional request configuration. By default we add token to ensure that the webhook request is legitimate

1 item

KEY	VALUE	
<input type="text"/>	<input type="text"/>	<input type="button" value="Remove"/>

[Add Header](#)

<input type="button" value="Cancel"/>	<input type="button" value="Save"/>
---------------------------------------	-------------------------------------

- In the Create Webhook dialog, complete the following fields:
 - Name:** Enter a unique name for the webhook to help identify it in your system.
 - Endpoint URL:** A URL of your Splunk Cloud instance.
 - Description:** Enter a brief description of the webhook to provide context about its specific function.
 - Webhook State:** Use the checkbox to enable or disable the webhook, where checking it makes the webhook active and unchecking it disables notifications.
 - Triggers:** Choose Service, Level, and Event Type for your webhook subscription to receive notifications and add the Target to triggers.
 - Key:** The name of the header you want to add. It serves as an identifier for the data you are sending in the header.
 - Value:** The value associated with the header key. Enter the Token Value created for HTTP Event Connector in Splunk Enterprise
- Provide other required details, then click **Save**.
- Verify the configured webhook on the Delinea Platform (see [Testing a webhook](#)).

For more information, see [Webhook Management](#).

Troubleshooting

Issue:

An SSL error as a result of the webhook test.

Solution:

Webhooks

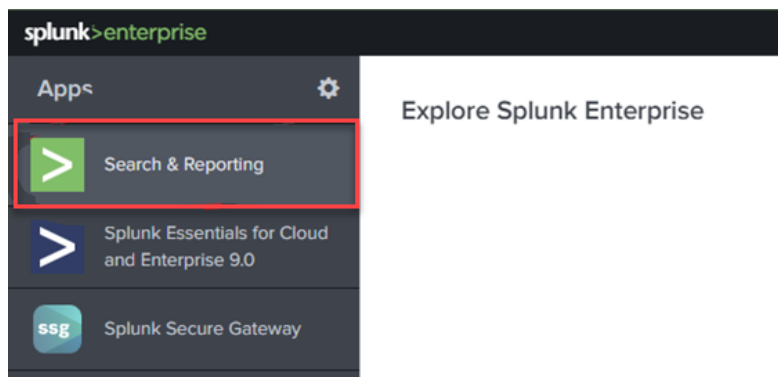
1. Depending on your operating system, open a terminal or a Command prompt.
2. Navigate to the Splunk directory on your computer and insert the following data:

```
var handler = new HttpClientHandler
{
    ClientCertificateOptions = ClientCertificateOption.Manual,
    ServerCertificateCustomValidationCallback =
        (httpRequestMessage, cert, cetChain, policyErrors) => true
};
```
3. Go back to the Delinea Platform and test the webhook created for Splunk Enterprise again.
4. Ensure that the webhook for Splunk Enterprise is configured correctly by receiving a success alert.

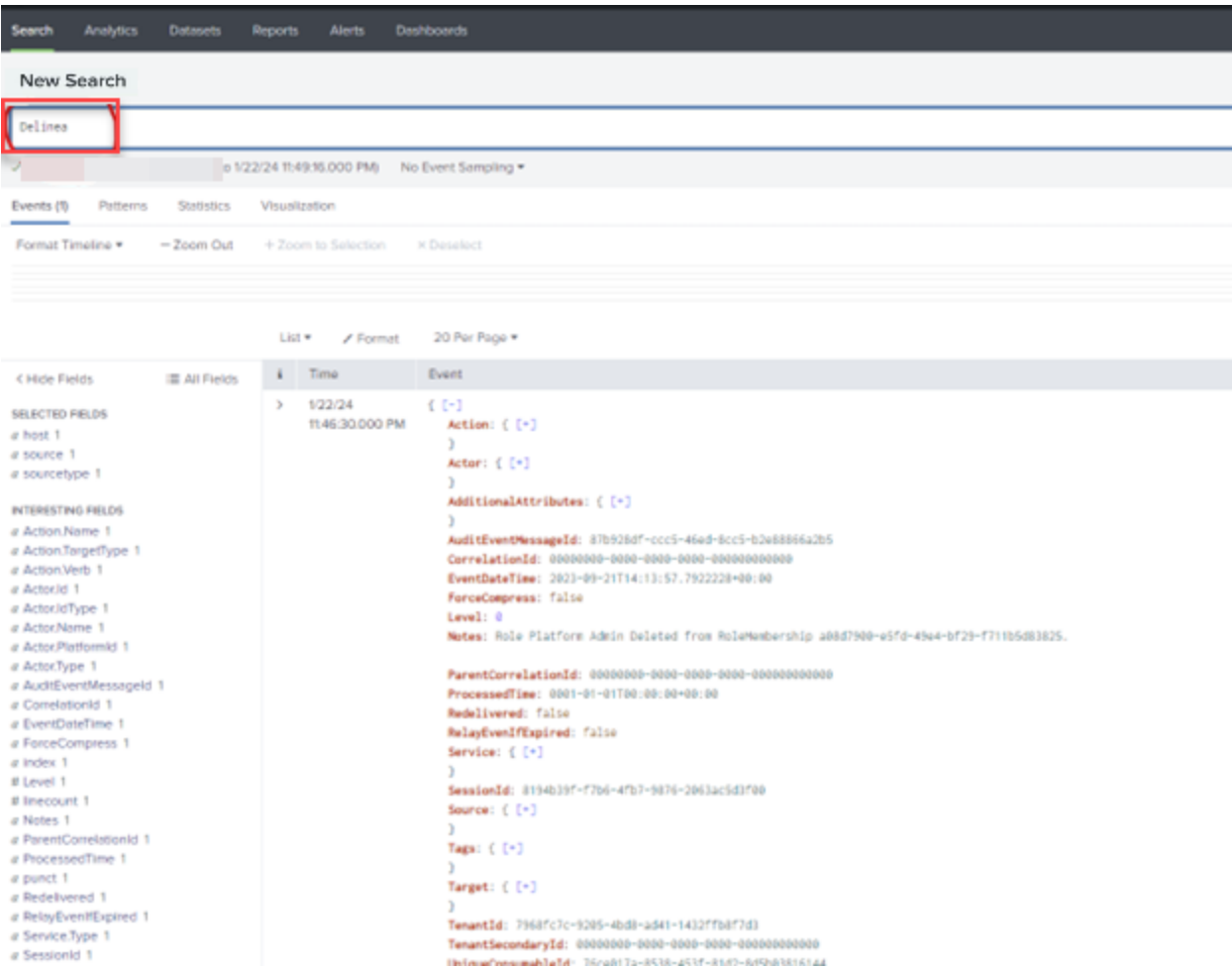
Verifying Logs for Splunk Webhook

When you have ensured that webhooks are correctly configured for Splunk Enterprise, you can verify that the expected logs were received using webhooks.

1. Log in to your Splunk Enterprise account with admin permissions.
2. From **Apps**, select **Search & Reporting**.



3. In **New Search**, specify "Delinea" and select **Enter**.
4. Verify that the log is displayed.



5. To verify the logs in the Delinea Platform see [Verifying a Webhook](#).

Integrating Splunk Cloud

Splunk Cloud is a cloud-based security orchestration, automation, and response system. It integrates security infrastructure orchestration, playbook automation, and case management capabilities.

You can integrate Splunk Cloud with the Delinea Platform by using webhooks.

Prerequisites

Ensure you have all the required accounts and utilities before starting the integration:

- Admin account with federation privileges on the Delinea Platform
- Admin account in [Splunk Cloud](#)

Configuring Splunk Cloud

To use the Splunk Cloud for integration, you must create an HTTP Event Collector, which allows you to send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols. For more

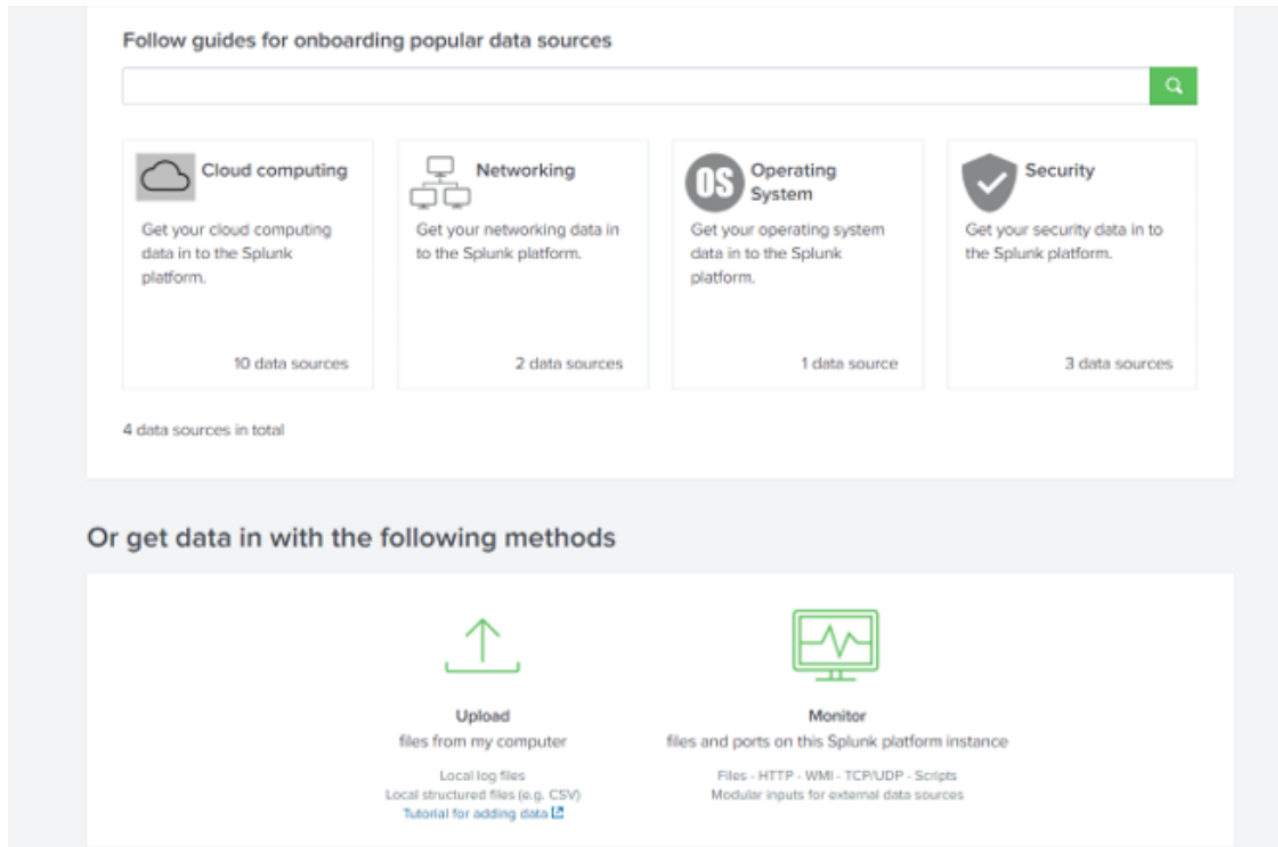
Webhooks

details, see [Splunk official documentation](#).

Creating an HTTP Event Collector in Splunk Cloud

To create an HTTP Event Collector:

1. Log in to Splunk Cloud as an Administrator.
2. Select the **Settings** tab then select **Add Data**.
3. Select **Monitor**.



4. In the dialog, select **HTTP Event Collector**.
5. Fill in the form for the new HTTP Event Collector.

Webhooks

Settings ▾Activity ▾Find 🔍

Add Data

< BackNext >

HTTP Event Collector

Configure tokens that clients can use to send data over HTTP or HTTPS.

Logd Input for the Splunk platform

This input collects data from logd on macOS and sends it to the Splunk platform.

Splunk Secure Gateway

Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

Splunk Secure Gateway Mobile Alerts TTL

Cleans up storage of old mobile alerts

Config Modular Input

Migrates configuration from conf file to KV store

Deep Link Dashboard Modular Input

Initializes the Deep Link Dashboard Modular Input to complete registrations

Splunk Secure Gateway Deleting Expired Tokens

Delete expired or invalid tokens created by Secure Gateway from Splunk

Splunk Secure Gateway Role Based Notification Manager

Used for sending mobile alerts to users by role

Configure a new token for receiving data over HTTP. [Learn More](#)

Name

Delinea platform

Source name override ?

optional

Description ?

Delinea platform webhook test

Enable indexer acknowledgement

☐

FAQ

> What is the HTTP Event Collector?

> How do I set up the HTTP Event Collector?

> How do I view and configure the tokens that I can use to send data to the HTTP Event Collector?

> What clients can send data to the HTTP Event Collector?

> What port and protocol does the HTTP Event Collector receive data on and how can I change that?

6. Click **Next > Preview**.

7. Verify the details for the newly created HTTP Event Collector and select **Submit**.

8. Go back to **Settings** and select **Data inputs**.

9. Choose your HTTP Event Collector and copy its token value.

splunkcloudApps ▾Messages ▾Settings ▾Activity ▾Find 🔍

Splunk Cloud Admin ▾Support & Services ▾

HTTP Event Collector

Global SettingsNew Token

Data Inputs > HTTP Event Collector

2 Tokens

App: All ▾filter 🔍

20 per page ▾

Name ▴	Actions	Token Value ▴	Source Type ▴	Index ▴	Status ▴
Delinea Platform	EditDisableDelete	CopyShow	*****	Default	Enabled
Webhooks	EditDisableDelete	CopyShow	*****	history	Enabled

Configuring Webhooks on the Delinea Platform

This section explains how to configure webhooks to work with Splunk Cloud. For more details about the concepts and general procedures in this section, see [Webhooks Management](#).

Creating a Webhook

To create a webhook:

Webhooks

1. Log on to the Delinea Platform.
2. From the left navigation menu, select **Settings > Webhooks**.
3. Select **Create Webhook**.

The Create Webhook dialog opens.

Create Webhook

Name

Endpoint URL

Description

Webhook State ☒ Enabled

Triggers

Subscribing your webhook to specific events allows you to receive notifications only for those events you are interested in

Service

Level

Event Type

Target

Custom Headers

Optional HTTP headers for additional request configuration. By default we add token to ensure that the webhook request is legitimate

1 item

KEY	VALUE
<input type="text"/>	<input type="text"/>

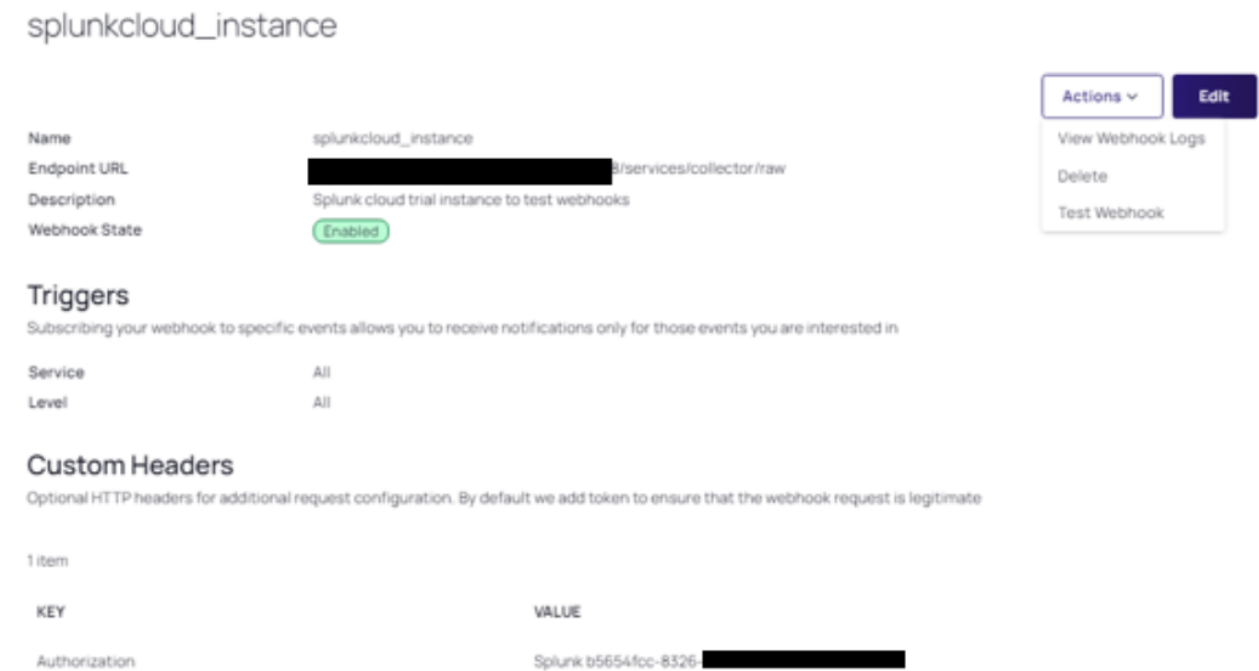
4. In the Create Webhook dialog, complete the following fields:
 - **Name:** Enter a unique name for the webhook to help identify it in your system.
 - **Endpoint URL:** A URL of your Splunk Cloud instance.
 - **Description:** Enter a brief description of the webhook to provide context about its specific function.
 - **Webhook State:** Use the checkbox to enable or disable the webhook, where checking it makes the webhook active and unchecking it disables notifications.
 - **Triggers:** Choose Service, Level, and Event Type for your webhook subscription to receive notifications and add the Target to triggers.
 - **Key:** The name of the header you want to add. It serves as an identifier for the data you are sending in the header.
 - **Value:** The value associated with the header key. It is the data you intend to send with the webhook request under the specified header key.
5. Provide other required details, then click **Save**.

Testing Webhooks on the Delinea Platform

You can test your webhook to verify that the destination URL is correct and the connection is successful.

To test a webhook:

1. From the left navigation menu, select **Settings > Webhooks**.
2. Open the webhook and select **Action > Test Webhook**.



Verifying Splunk Cloud Integration with the Delinea Platform

To confirm that the first connection between the services is successful, you can generate log files and check the integration of the Splunk Cloud and Delinea Platform.

Verifying Integration in Splunk Cloud

To verify Delinea Platform integration with Splunk Cloud:

1. Log in to the Splunk Cloud as an Administrator.
2. In the **Search** field, enter a query as `index=*`.
3. Select the search icon to verify logs from the platform.

You should see the latest log files.

Verifying Integration on the Delinea Platform

Based on a webhook test result, you can check the log files. For more details, see [Webhooks Logs](#).

Integrations and Marketplace

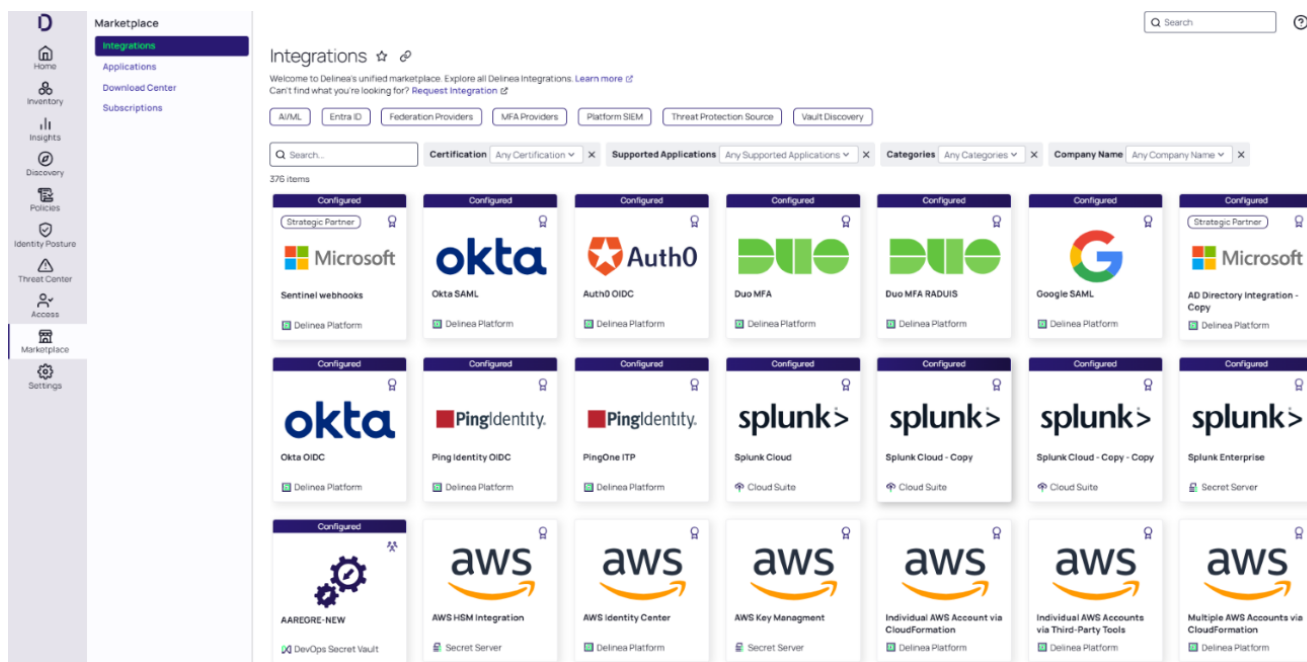
The Delinea Marketplace is an integration ecosystem for shared services where you can find applications, scripts, utilities, and other software you can use with Delinea products. By default, the Platform Admin controls Marketplace access permissions for users.

Integrations

The Delinea Marketplace Integrations page houses Delinea built-in product integrations, plug-ins and utilities, as well as third-party solutions compatible with the Delinea ecosystem. This page offers a vast collection of pre-built integrations that connect your Delinea system solution to a wide range of other tools and applications. These integrations streamline workflows, automate tasks, and enhance your overall security. From SIEM and IAM integrations to custom connectors for industry-specific applications, you'll find the perfect solution to expand the capabilities of your Delinea Platform.

To display the available integrations, select **Marketplace > Integrations** from the left navigation menu. If an integration has an associated configuration for your Delinea Platform tenant, a **Configured** banner is displayed along the top of the integration card. You can view the configuration from the integration details. See "Integration Details" on page 589.

You can search for integrations by using the Search box or one of the filtering options at the top of the Integrations page to filter your results. For more information, see "Sorting" below.



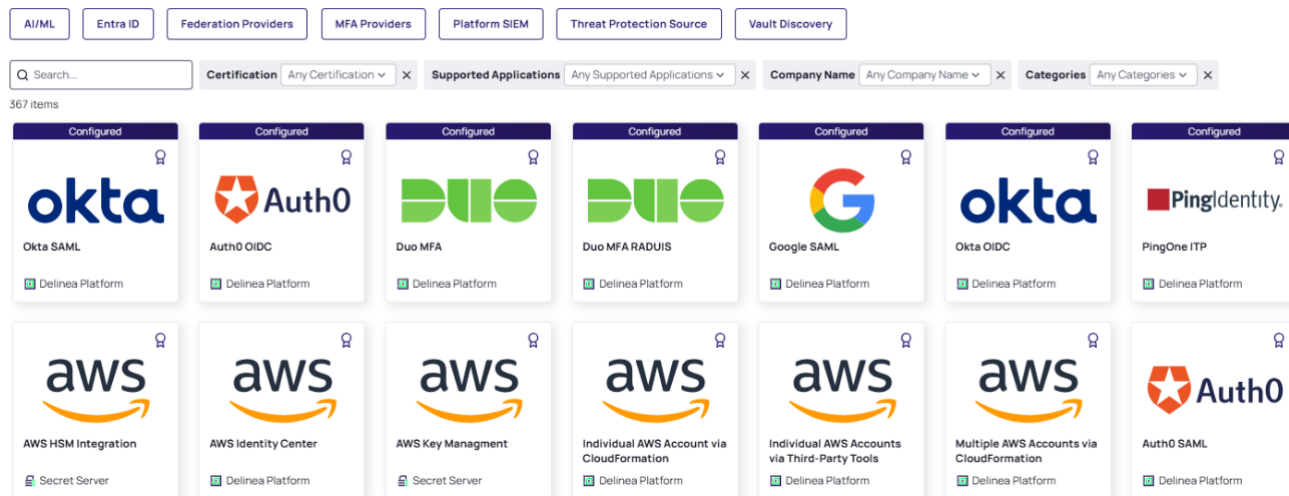
Sorting

The cards for configured integrations are prominently shown at the top of the Delinea Marketplace Integrations page, providing a clear and concise overview of all connected systems. Other integration cards are sorted alphabetically.

Integrations and Marketplace

Integrations ☆ ↗

Welcome to Delinea's unified marketplace. Explore all Delinea Integrations. [Learn more](#) ↗
Can't find what you're looking for? [Request Integration](#) ↗



Filtering Options

You can filter the integrations by **Certification** status, compatible Delinea **Supported Application**, vendor **Company Name**, or **Category**, and you can select multiple options within each category.

■ Certification:

- **Contributed Integration:** A third-party vendor developed and maintains this integration. Delinea cannot guarantee its proper functioning or compliance with Delinea product limitations. Delinea has not reviewed or supported this integration.
- **Delinea Certified:** Delinea supports this integration and has verified and documented its compatibility with the specified Delinea product.
- **Delinea Community:** Integrations provided by the community are not guaranteed to be error-free or to function as intended. You are responsible for thoroughly testing the scripts before using them in any environment. Please note that the provided scripts may be subject to change without notice.
- **Delinea Trusted:** A third-party vendor developed and maintains this integration. Delinea has reviewed its compatibility; however, for ongoing support, please refer to the third-party vendor's documentation or support channels.

■ Supported Applications:

Integrations compatible with products provided and fully supported by Delinea. These include Cloud Suite, the Delinea Platform, DevOps Secrets Vault, Privilege Manager, Secret Server, and Server Suite.

■ Company Name:

Finds integrations from specific vendors.

■ Categories:

Sorts and finds integrations based on specific functionalities or areas of focus. Each category represents a different aspect of security or IT management.


Integration Details

When you open an individual integration card, you see a description on the right and a narrower information panel on the left.


The information panel displays the following:

- A logo or icon related to the offering.
- A **Configure** button, a **Download** button, or a **View Configuration** button.
- **Supported Application(s)**: the applications developed and supported by Delinea that are compatible with the integration you are looking at.
- **Categories**: the type(s) or purposes of the integration.


The **Configure** button is available for native platform integrations. Select it to display a page where you can set up and manage the Delinea Platform integration.


[Configure](#)


Amazon - Individual AWS Accounts via Third-Party Tools

Developed by Delinea  Delinea Certified

Integrating AWS with the Delinea Platform enables Privilege Control for Cloud Entitlements (PCCE) so you can discover identities, groups, and assets on your AWS account. AWS can be integrated for specific accounts or an entire organization, and your integration can also include the IAM Identity Center. Integrating Individual AWS Accounts (via 3rd Party tools) enables you to create a role for each account and allows a platform user to access the role.

[Learn More](#) 

Supported Application

 Delinea Platform

Categories

Cloud Infrastructure
Entitlement Management
(CIEM)

Privilege Control for Cloud
Entitlements (PCCE)

Cloud Identity Discovery

The **Download** button is available for the Delinea plug-ins. Select it to get the files needed for the integration, such as a plugin or connector.

Integrations and Marketplace



Microsoft - Sentinel Syslog AMA

Developed by Delinea [Strategic Partner](#) [Delinea Certified](#)

The integration between Microsoft Sentinel and Secret Server combines powerful security event monitoring and analytics with robust privileged access management capabilities. It enhances threat detection, incident response, and compliance, while providing organizations with greater visibility and control over privileged access to critical systems and data. Effortlessly ingest Syslog messages from your Linux machines, devices, and appliances directly into Sentinel. No more managing complex log forwarders – the Azure Monitor Agent (AMA) takes care of everything.

[Learn More](#)

Supported Application

Secret Server

Categories

Security Information and
Event Management (SIEM)

The **View Configuration** button is available for native platform integrations that have an associated configuration for your Delinea Platform tenant. Select this button to view the configuration on the platform.



Okta - Okta OIDC

Developed by Delinea [Delinea Certified](#)

Okta is a leading identity and access management platform that provides secure single sign-on (SSO) and authentication services. Integrating Delinea Platform with Okta SAML enables organizations to centralize user authentication and access control for Delinea Platform using Okta as the identity provider.
The Delinea Platform currently supports two authentication protocols: Open ID Connect (OIDC) and Security Assertion Markup Language (SAML). An external federated identity provider can be configured on the platform to use either protocol, depending on what the provider supports and on what you want to do. Delinea Platform integrates with Okta SAML using federation service. When a user initiates log-in, the platform checks the domain name of the user ID. If the domain is configured for an external federated IDP, the log-in data is passed to Okta, and the user is authenticated and logged in.

[Learn More](#)

Supported Application

Delinea Platform

Categories

OpenID Connect (OIDC)
Identity Management
Identity and Access
Management (IAM)
Single Sign On (SSO)

The **Learn More** link is available for the selected integration. Select it to open the documentation for that integration.

Applications

To display the available applications, select **Marketplace > Applications** from the left navigation menu.

The Applications page displays software products and solutions developed and fully supported by Delinea.

To find specific applications, use the **Search** box or the filters to the right of the Search box. For more information, see "Filtering in List Pages" on page 48.

The filters for Delinea Applications are organized into three categories.

Group:

- **Delinea Applications:** Applications developed by Delinea.
- **Delinea Products and Services:** A broader range of Delinea offerings, including services
- **Delinea Tools:** Tools provided by Delinea.

Supported Applications: Delinea products compatible with the offerings on the Applications page.

Categories: With the Categories filter in the Delinea Applications Marketplace, you can sort and find applications based on specific functionalities or areas of focus. Each category represents a different aspect of security or IT management.

Application Details

To view the details of an application, select **Marketplace > Applications** from the left navigation, then select the card for the application you want to see.

When you open an application card, one of the following buttons is displayed: **Download**, **Configure**, or **Start Trial**.

The **Download** button is available for the Delinea applications. Select it to get the necessary files to download the application.



Download

Supported Application

 Delinea Platform

Categories

Session Management

Delinea - Connection Manager

Developed by Delinea

Connection Manager is Delinea tool that helps organizations to improve the security of their connections to remote systems. With Delinea Connection Manager, IT teams can launch ad-hoc connections to manage sessions with remote resources, navigating Remote Desktop Protocol (RDP) and Unix Secure Shell (SSH) connection protocols as needed. Management of multiple active sessions is easy. You can store and organize connections by adding them to your favorites and import any folder structure or connections used in other tools for a single management hub.

It marks an expansion of Delinea's product line to include remote connectivity tools closely integrated with Secret Server. It permits technical staff to quickly access resources using the convenience of a familiar, rich desktop interface while maintaining all the safeguards and workflows included with Secret Server.

Connection Manager is a desktop client application that can be downloaded and installed on Windows and Mac machines. Connection Manager provides a number of features that can help to reduce the risk of unauthorized access, data loss, and fraud. It offers a wide range of features, including:

- **Centralized management:** Connection Manager provides a central location for administrators to manage all of their connections. This can help to reduce the risk of unauthorized access to sensitive systems and data.
- **Secure storage:** Connection Manager stores connections in an encrypted format, protecting them from unauthorized access.
- **Single sign-on:** Connection Manager supports single sign-on, which allows users to sign in to multiple systems with a single set of credentials. This can help to reduce the risk of password fatigue and password reuse.
- **Multi-factor authentication:** Connection Manager supports multi-factor authentication, which adds an additional layer of security to connections. Multi-factor authentication requires users to provide two or more pieces of evidence to authenticate themselves, such as a username, password, and security code.
- **Session recording:** Connection Manager supports session recording, which allows administrators to record user sessions. This can be helpful for troubleshooting problems and for auditing user activity.
- **Compliance reporting:** Connection Manager supports compliance reporting, which allows administrators to generate reports on user activity. This can be helpful for organizations that need to comply with security regulations.


[Learn More](#) 

The **Configure** button is available for native Delinea Platform applications or services. Select it to access the management interface for that application.



Configure

Delinea - Delinea Authenticator

Developed by Delinea  Delinea Certified

Delinea Authenticator mobile app provides quick and easy access to TOTP codes and multi-factor authentication (MFA) push notifications. The application also supports biometric data to make the user experience convenient and secure. Registration can be completed for one or more Delinea Platform tenants by simply scanning the QR code under the Applications tab in your User Profile

[Learn More](#) 

Supported Application

 Delinea Platform

Categories

Identity and Access
Management (IAM)

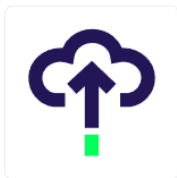
Multi-Factor Authentication
(MFA)

Single Sign On (SSO)

Privileged Access
Management (PAM)



The **Start Trial** button is displayed if the full version is not yet available.



Start Trial

Supported Application

 Cloud Suite

Categories

Endpoint Security and Management

Privileged Access Management (PAM)

Delinea - Cloud Suite

Developed by Delinea

Cloud Suite is a comprehensive suite of cloud-based solutions that provides organizations with a range of tools and capabilities to enhance their cybersecurity and identity and access management (IAM) practices. It offers various modules and components that address critical aspects of security and access control within an organization's IT infrastructure.

Cloud Suite is a cloud-based application designed to work with other applications such as Privilege Access Service (PAS) to provide a comprehensive business solution. PAS includes a privileged identity management service that can manage passwords and account information for systems, domains, databases, services, and secret text strings or files that contain secret information. You can deploy PAS using cloud-based services or PAS on-site in your network, in a private cloud, or in a public cloud instance you manage. You can deploy PAS with passwords managed securely using the Delinea cloud-based platform or onsite deployment, using a key management appliance such as SafeNet KeySecure. You can also use an infrastructure of your choice, such as an internal firewall-protected network, a private cloud, or a public cloud instance such as Amazon Web Services.

Cloud Suite Keynotes:

- **Privileged Access Management (PAM):** Cloud Suite includes robust privileged access management capabilities, allowing organizations to secure and manage privileged accounts and access to critical systems. It offers features such as password management, session recording, access controls, and auditing to ensure privileged accounts are protected and monitored effectively.
- **Identity and Access Management (IAM):** Cloud Suite provides comprehensive IAM functionalities, enabling organizations to manage user identities, access controls, and user lifecycle processes. It supports centralized user provisioning, role-based access control (RBAC), self-service password reset, and multi-factor authentication (MFA) to ensure secure and efficient user access management.
- **Secure Password Management:** Cloud Suite offers secure password management features, allowing organizations to securely store and manage passwords for privileged accounts and other sensitive credentials. It includes capabilities such as password rotation, password complexity enforcement, and secure password sharing, reducing the risk of password-related security incidents.
- **Governance and Compliance:** Cloud Suite incorporates governance and compliance features to help organizations meet regulatory requirements and internal policies. It offers access request workflows, access certifications, and compliance reporting capabilities, ensuring that access rights are granted based on business justifications and regularly reviewed for compliance.
- **Integration Capabilities:** Cloud Suite is designed to integrate with various IT systems and applications, allowing organizations to leverage existing infrastructure investments. It offers integrations with popular technologies such as Active Directory, SIEM platforms, ticketing systems, and cloud service providers, enabling seamless data exchange and enhancing overall security posture.
- **Reporting and Analytics:** Cloud Suite provides comprehensive reporting and analytics capabilities to gain insights into privileged access activities, user behavior, and compliance status. It offers customizable dashboards, audit trails, and real-time monitoring, empowering organizations to make informed security decisions and identify potential security risks.
- **Cloud Deployment:** As the name suggests, Cloud Suite is a cloud-based solution, offering the benefits of scalability, flexibility, and ease of management. It eliminates the need for on-premises infrastructure and allows organizations to leverage the advantages of cloud computing, including rapid deployment, automatic updates, and high availability.

[Learn More](#) 

Quick Filters

Quick Filters are predefined filter options that let you quickly filter the marketplace listings. Quick filters appear at the top of the Integrations page or the Applications page. When you select a quick filter, only the marketplace cards that are associated with that quick filter are displayed (as shown in the image below).



Note: You can select only one quick filter at a time to filter the marketplace cards.

Integrations and Marketplace

Integrations ☆ ↗

Welcome to Delinea's unified marketplace. Explore all Delinea Integrations. [Learn more](#) ↗
Can't find what you're looking for? [Request Integration](#) ↗

AI/ML

Cloud Security

Entra ID

ITSM

MFA

SCIM

SIEM

SSO

ServiceNow

Splunk

Terraform

Q Search...

Certification Any Certification ▾ ×

Company Name Any Company Name ▾ ×

Categories Any Categories ▾ ×

Supported Applications Any Supported Applications ▾ ×

15 items

aws

AWS Identity Center

Delinea Platform

aws

Individual AWS Account via CloudFormation

Delinea Platform

aws

Individual AWS Accounts via Third-Party Tools

Delinea Platform

aws

Multiple AWS Accounts via CloudFormation

Delinea Platform

citrix

Linux VDA Smartcard

Server Suite

Strategic Partner

Microsoft

Entra ID (ITP)

Delinea Platform

Strategic Partner

Microsoft

Entra ID (PCCE)

Delinea Platform

citrix

Linux VDA

Server Suite

Strategic Partner

Microsoft

Defender for Identity

Secret Server

okta

Okta ITP

Delinea Platform

ORACLE

Oracle Cloud

Fastpath Access Control

ORACLE

Oracle Cloud

Fastpath Change Tracking

PingIdentity

PingOne ITP

Delinea Platform

Snowflake (ITP)

Delinea Platform


workday

Workday ITP

Delinea Platform

To find the marketplace cards you want, you can use quick filters in combination with search and the filter options for Categories, Certification, Company Name, and Supported Applications.

Download Center

 **Note:** The Download Center has its own permission system, so administrators can control a user's access to the Download Center, whether the user does or does not have Marketplace permissions.

The Download Center displays software packages for the Delinea Platform, developed and fully supported by Delinea. These include agents, connectors, remote access software, tools, and updates.

Use the **Learn More** link to access the Delinea Platform Marketplace documentation and explore its functionalities.

You can use the **Search** box to find the package you need or use the filter menu to display the packages by category, architecture, or operating system.

To view the Download Center, select **Marketplace > Download Center** from the left navigation.

Integrations and Marketplace


The screenshot displays the Delinea Download Center interface. On the left is a sidebar with navigation icons and labels: Home, Secret Server, Inventory, Insights, Discovery, Policies, Identity Posture, Threat Center, Access, Marketplace, Inbox, and Settings. The main content area is titled 'Download Center' and includes a search bar, a 'Filters' panel on the left, and a table of 42 items. The table has columns for NAME, CATEGORY, VERSION, OPERATING SYSTEM, and RELEASE DATE. The first row is highlighted, showing 'Active Directory Connector' (Connector, 6.1.920, MS Windows, 10/2/24). To the right of the table is a preview pane for the 'Active Directory Connector', showing its category, version, operating system, architecture, release date, and a description.

NAME	CATEGORY	VERSION	OPERATING SYSTEM	RELEASE DATE
Active Directory Connector	Connector	6.1.920	MS Windows	10/2/24
Connection Manager	Remote Access	2.5.3	MS Windows	9/30/24
Connection Manager	Remote Access	2.5.3	MacOS	9/30/24
Privilege Control for Servers Agent (.apk)	Agents	2024.0.3 (6.1.0)	Alpine Linux	8/21/24
Privilege Control for Servers Agent (.deb)	Agents	2024.0.3 (6.1.0)	Ubuntu Linux	8/21/24
Privilege Control for Servers Agent (.deb)	Agents	2024.0.3 (6.1.0)	Ubuntu Linux	8/21/24
Privilege Control for Servers Agent (.deb)	Agents	2024.0.3 (6.1.0)	Debian Linux	8/21/24
Privilege Control for Servers Agent (.gz)	Agents	2024.0.3 (6.1.0)	IBM AIX Unix	8/21/24
Privilege Control for Servers Agent (.gz)	Agents	2024.0.3 (6.1.0)	Hewlett Pack	8/21/24
Privilege Control for Servers Agent (.msi)	Agents	2024.0.3 (6.1.0)	MS Windows	8/21/24
Privilege Control for Servers Agent (.p5p)	Agents	2024.0.3 (6.1.0)	Oracle Solar	8/21/24
Privilege Control for Servers Agent (.p5p)	Agents	2024.0.3 (6.1.0)	Oracle Solar	8/21/24
Privilege Control for Servers Agent (.rpm)	Agents	2024.0.3 (6.1.0)	Red Hat Ente	8/21/24

The Download Center grid displays key information about each asset, with customizable columns so you can adjust the display to suit your preferences. You can add columns from the list below, or remove columns as needed.

- **Name:** The name of the software or tool available for download.
- **Category:** The classification of the item, such as Connector, Remote Access, or Agents.
- **Version:** The version number of the software, indicating its release iteration.
- **Operating System:** The operating system(s) that the software is compatible with, such as MS Windows, MacOS, or various Linux distributions.
- **Architecture:** The hardware architecture the software supports.
- **Release Date:** The date the software version was released or made available for download.
- **Description:** A brief explanation of the software's functionality or key features.

Click anywhere in a row to open a preview pane on the right side, displaying a description and other details about the package. Select the **Download** link in the preview pane to download the selected software package to your computer.

 **Note:** The Download icon is also shown next to the application name on the Download Center page, so you can download the selected software package to your computer.

Select the **View Release Notes** link in the preview pane to go to a web page with the release notes for the software or tool or download the release notes document.

If any older versions of the software package are available for download, those versions appear under Previous Versions, as shown in the image below. To download an older version of the package to your computer, select the download icon next to the version number. To verify that an older version's download file is valid, use the SHA-256 and SHA-512 checksums below the version number. To copy a checksum to the clipboard, hover over the right end

of the checksum string until a copy icon appears and then select it.

Connection Manager

X

Download

View Release Notes 

Overview

^

Category

Session Managment

Version 2.5.4




SHA256	e19b6b66bb18...
SHA512	f6c52e912ef9...

Architecture

x64

Operating System

 MS Windows

Release Date

12/5/2024

Description

Includes vault auto-reauthentication configuration, machine field display, and memory leak improvements

Previous Versions

^

Version 2.5.3



Delinea Delinea Platform	Administrator Guide
SHA256	e19b6b66bb18...
SHA512	f6c52e912ef9...

To download the package, hover your cursor to the right of the package name and click the download icon.

To filter the packages displayed, click the filter icon to the left of the Search box. The downloads in the Download Center can be filtered in the following ways:

- **Architecture:** Software packages compatible with specific hardware platforms and configurations.
- **Operating System:** Software package compatible with specific operating systems, including various MS Windows, MacOS, Unix, and Linux distributions.
- **Category:** Software package of different types and purposes, including Agents, Connector, Guide, Installer, Remote Access, and Tools.

Mobile Access

Most functions related to mobile access are available through the [Delinea Mobile](#) application installed on a consumer's mobile device. After a user of the Delinea Mobile application logs in for the first time and registers their device, administrators of the Delinea Platform can view the device and its settings by following the steps below under **Administrators**.

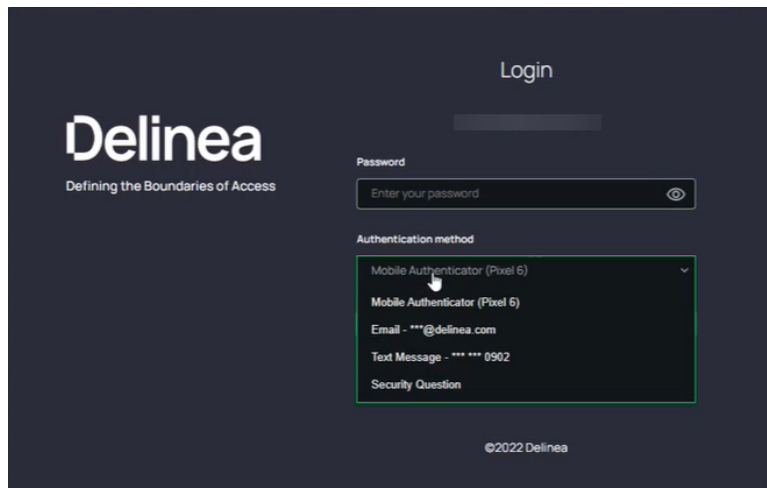
For additional information on the Delinea Mobile application and using it to log into the platform using MFA, see the following: [Delinea Mobile Overview](#), [Delinea Mobile Log in Process](#), [Delinea Mobile Login Flow](#).

Administrators

1. Click **Settings** in the left navigation, then select **Authentication Profiles**.
2. Click the **Security devices** tab. Each device registered for mobile access will appear in a row, with columns displaying the **Device Name**, **Model Name**, **Client Version**, **User**, and **User Status**.

Users

If an administrator has set up MFA as an option for a user, and has set one of the available authentication methods to be performed on a mobile device, the user will see each of their registered mobile devices on the login screen under **Authentication Method**. The device name appears in parentheses after **Mobile Authenticator**.



Platform Notifications

To receive notifications from the platform on a mobile device, a user must first log in to the platform at least once from the device. This first login registers the user's mobile device to the user's profile. The user can then receive and reply to notifications, such as login MFA challenges, even when they are not logged in to the mobile application.

A device can be registered to only one platform user profile at a time. If a different user subsequently logs in to the same platform tenant from the same registered device, the device will be removed from the original user's profile. The original user will no longer be able to receive notifications from the platform.

If a user no longer wishes to receive notifications on a device, they must log in to their platform tenant, go to their profile, and delete the device from their list of registered devices.

Authenticating with Platform APIs

Please click the link to view the content on [Authenticating with Platform APIs](#).



Note: Secret Server has its own, separate API. See [Using Secret Server APIs from Delinea Platform](#).

Privilege Control for Servers

Privilege Control for Servers (PCS) brings Delinea's Privileged Access Management (PAM) capabilities to the servers and computer endpoints in your corporate network. Typically, before starting to use PCS, you would have a standard environment and components already deployed for the Delinea Platform and Secret Server.

This page gives a brief description of the services provided by PCS. They are explained in more depth in the rest of this documentation.

The Privilege Control Agent

On non-Windows computers, Privilege Control for Servers consists of the core Privilege Control Agent (adclient), related libraries, and optional tools. The Privilege Control Agent enables local host computers—most commonly Linux or UNIX—to join an Active Directory domain. After the agent is deployed on a server, that computer is considered a *managed computer*, and it can join any Active Directory domain you choose.

When a PCS-managed computer joins an Active Directory domain, the computer essentially becomes an Active Directory client. It relies on Active Directory and the Delinea Platform to provide authentication, authorization, policy management, and directory services. The interaction between Active Directory and the agent on the local computer is similar to the interaction between a Windows system and its Active Directory domain controller, including failover to a backup domain controller if the managed computer cannot connect to its primary domain controller.

PCS Policies

PCS policies provide users with machine-level (server) permissions for logging in to remote computers and servers managed by Delinea Platform and performing elevated actions on them. By assigning machine-level policies, you can ensure that each asset adheres to compliance standards, maintaining both security and efficiency across your network.

Inventory

The Inventory service delivers a user-friendly, asset-centric perspective of computers within your infrastructure. It empowers the user to readily view and manage assets, and to launch remote sessions directly on computers that have been discovered through the Secret Server discovery service.

Engine Management

The Delinea Platform manages and protects endpoints using small software packages called engines. The platform's Engine Management feature provides administrators with a single interface for managing these engines, which are automatically updated and maintained after installation – removing the need for separate installers and management processes that are traditionally necessary on individual machines. See [Engine Management](#).

Audit Collector


Audit Collectors transmit machine-level audit data to the Delinea Platform, so recorded activities and events can be presented and examined. The Audit Collectors function as intermediary services that receive and compress activities captured in real time from agents deployed on audited computers.

An agent on each audited machine captures user activities and forwards them to a designated Audit Collector. When the agent cannot establish a connection with a collector—for example, when computers hosting the collector service are offline for maintenance—the agent temporarily stores the session data locally, then transfers it to a collector once the connection is reestablished. The collector then transmits this data to the Delinea Platform.

We recommend setting up at least two Audit Collectors to ensure uninterrupted auditing. Additional collectors can be deployed at any point for additional resiliency or improved scale. See [Audit Collector Workload](#).

Command Relay

The Command Relay facilitates communication between the Delinea Platform and your environment through an SSH connection. Its primary function is to dispatch commands along with their parameters to be executed within your environment. The Command Relay requires a service account that can modify your domain so the proper administrative policies can be added.

 **Note:** PCS does not support FIDO2 MFA.

Next Steps

For information about how to install and set up PCS, see "Setting Up PCS" below.

Setting Up PCS

This section tells how to install, configure, and start using Privilege Control for Servers (PCS).

For an overview of PCS and its components, see "Privilege Control for Servers" on the previous page.

Prerequisites to PCS Installation

Before you start installing and using PCS, you must already have the Delinea Platform set up for fundamental tasks.

Follow these procedures and understand these concepts:

- "Using Platform Integration Center" on page 777
- "Discovery" on page 165 for Active Directory users and servers
- "Setting Up a PRA Engines Site" on page 293
- "Installing PRA Engines" on page 301
- "Installing the Delinea Connector" on page 272
- "Creating Authentication Profiles" on page 473
- "Vaulting Secrets on the Platform" on page 91 (including how to place an account in the Secret Server vault)

PCS Installation Overview

To set up Privilege Control for Servers to work on the Delinea Platform and start using it, perform the following tasks:

"Step 1: Configure Firewall Ports for PCS" on the next page

"Step 2: Set Up PCS Service Accounts" on the next page

"Step 3: Install the Delinea Connector on Managed Servers" below

"Step 4: Enable IWA Service on Connectors" below

"Step 5: Install the Delinea Platform Engine on Managed Servers " below

"Step 6: Install the Delinea Agent on Managed Servers" on page 604

"Step 7: Scan Computer Inventory" on page 608

"Step 8: Set Up Authentication Profiles for PCS" on page 608

"Step 9: Set Up PCS Policies" on page 608

"Step 10: Set Up Audit and Session Recording" on page 608

"Step 11: Set Up Use My Account" on page 610

Step 1: Configure Firewall Ports for PCS

To use Privilege Control for Servers, be sure your firewall ports are configured appropriately. Use the procedure in [Customer Firewall Requirements](#).

Step 2: Set Up PCS Service Accounts

On the Delinea Platform, create a domain service account with roles and permissions that are specific to PCS. This account is called a Command Relay Service Account. The account must be placed in the Secret Server vault to be used for setting up Delinea Platform Engine Management and its Command Relay workload (see "Command Relay Workload" on page 259).

You must create at least one of these accounts, but you can also create more according to best practices for the Secret Server Discovery and Directory Services.

See also "Platform Engine Management" on page 233 and "Roles and Permissions" on page 203.

Step 3: Install the Delinea Connector on Managed Servers

The Delinea Directory Connector enables secure communication between the Delinea Platform and AD directories. Install the Delinea Connector on your target servers by following the procedures under "Active Directory Connector" on page 271 and in these sections:

- "Installing the Delinea Connector" on page 272
- "Using Connector Best Practices" on page 283
- "Troubleshooting the Delinea Connector" on page 287

Step 4: Enable IWA Service on Connectors

Enable Integrated Windows Authentication for PCS by following the procedure at "Configuring IWA" on page 505.

Step 5: Install the Delinea Platform Engine on Managed Servers

Delinea Platform Engine and Engine Management are components of the larger Delinea Platform product, and they are required by Privilege Control for Servers. The Delinea Platform Engine runs two workloads for PCS:

- Command Relay
- Audit Collector

To install the Delinea Platform Engine:

1. On the server where the Delinea Platform Engine will be running, along with its Command Relay and Audit Collector workloads, log in as a user with the custom role you created for viewing inventory.
2. Download and install the Delinea Platform Engine on your target servers by following the procedures in "Platform Engine Management" on page 233.

Updating the Platform Engine Management Settings

After installing the Delinea Platform Engine on your target servers, adjust the engine management settings.

1. From the left navigation, select **Settings**, then **Engine Management**.
2. Select the site that you want to update using the vaulted secret you just created.
3. Click the **Settings** tab.
4. Next to Audit Collector, click **Edit**.
5. Enter the following settings:
 - Collector Port: 5063
 - Session Recording: enabled
6. Click **Save**.
7. Next to Command Relay, click **Edit**.
8. Next to Command Relay Service Account, click **Select**.
9. Search for and select the vaulted engine management account you created earlier.
10. Click **Turn off folder inheritance and share secret**.
11. Click **Save**.

Updating the Platform Engine

The Delinea Platform Engine version 1.2.33.0 or later is required for PCS. You might need to update the software version for your Delinea Platform Engine.

1. Click **Settings**, then click **Engine Management**.
2. Click the name of the site where your Delinea Platform Engine is installed.
3. Click the **Engines** tab.
4. Look at the Version column.

If the version is not 1.2.33.0 or later, update the engine as follows:

1. In the Engines tab, click the name of the engine.
2. Click the **Workloads** tab.

3. In the Command Relay row, look at the Version column.
4. If the version is not 1.0.94 or higher, restart the Delinea Platform Engine service on the server that is running the Delinea Platform Engine. Wait for Command Relay to update.
5. Log in to the server running the Delinea Platform Engine.
6. Open PowerShell as an administrator.
7. Copy the following script:

```
Clear-Host;Write-Host "Uninstalling Delinea Platform Engine"; $ZipFile =
"$env:TEMP\DelineaEngineInstaller.zip"; $InstallerFolder = "$env:TEMP\$($New-Guid)";
$ProgramFilesFolder = 'C:\Program Files\Delinea Platform Engine'; $ProgramDataFolder =
'C:\ProgramData\Delinea Platform Engine'; $ProgressPreference = 'Continue'; Write-Host
"Downloading latest installer packages. This may take a moment..."; if (Test-Path
$ZipFile) { Remove-Item $ZipFile } if (Test-Path $InstallerFolder) { Remove-Item
$InstallerFolder -Recurse -Force } $Uri =
'https://enginepoolupdatedev.blob.core.windows.net/shell-installer/555173/win-x64.zip'; if
($PSVersionTable.PSVersion -lt [Version]"6.0") { $ProgressPreference = 'SilentlyContinue'
} Invoke-WebRequest $Uri -OutFile $ZipFile; $ProgressPreference = 'Continue'; Expand-
Archive $ZipFile $InstallerFolder; Remove-Item $ZipFile; Set-Location -Path
$InstallerFolder; ./Delinea.EnginePool.Engine.Installer.exe uninstall --keep-working-
directory; if (Test-Path $ProgramFilesFolder) { Remove-Item -Recurse -Force
$ProgramFilesFolder; } if (Test-Path $ProgramDataFolder) { Remove-Item -Recurse -Force
$ProgramDataFolder; }
```

8. Paste the script into PowerShell.
9. Run the script.



Note: If errors happen during the uninstall, close the PowerShell windows, launch PowerShell again as administrator, and run the uninstall script.

10. On the Delinea Platform, click **Settings**, then click **Engine Management**.
11. Open the site where the Delinea Platform Engine is installed.
12. Click the **Engines** tab.
13. Click the engine name.
14. Click **Delete Engine**.

Step 6: Install the Delinea Agent on Managed Servers

Now that you have installed the Delinea Platform Engine, install the Delinea Agent on your managed servers.

Requirements for Delinea Agent Installation

Before you begin installing and setting up the Delinea Agent:

- Make sure the servers where the Delinea Agent will be installed are using one of the supported operating systems. See "Supported Operating Systems for Agents" on page 610.
- Before running the procedures in this section, we recommend you see the additional content at "Managing Agents" on page 645.

Checking for Agent Installation

To see whether the Delinea Agent is already installed on a given computer, view the computer's information in the Inventory page. See "Inventory" on page 96.

If the agent is installed, the Client Version field shows a software version number. You can skip the next few procedures for downloading and installing the agent, because the agent is already present. Go ahead to "Step 7: Scan Computer Inventory" on page 608.

Downloading the Agent

To download the agent software:

1. Log in to your Delinea Platform tenant.
2. From the left navigation, select **Marketplace**, then **Download Center**.
3. In the Search box, enter **Agent**.
4. Find the agent for your operating system.
5. Click the download icon.
6. Wait for the package to compile and download.
7. Copy the download package to the server you want to manage.

Installing the Linux Agent

To install the Delinea Agent on a managed server that is running the Linux operating system, use the steps in this section.

To get more details about the Linux agent, see "Managing Agents " on page 645.

Requirements:

- Perl (and the following modules: lib, File::Basename, File::Copy, File::Find, File::stat, Getopt::Long, Sys::Hostname and Text::ParseWords)
- Forward and Reverse DNS entries for each *nix server



Note: If you require a different version of the *nix agent, visit the following site:

<https://<tenant>.delinea.app/view/marketplace/browse/authorization/agent-downloads-grid>



Note: You can also update the agent installation script to use the new URL for the agent download.

Steps:

1. Log in to your Linux server as root user.
2. Create a folder (for example, delinea-agent) and extract the package that you downloaded in "Downloading the Agent" above:

```
# mkdir delinea-agent
# tar -xzf rhel6-x86_64.tgz -C delinea-agent/
```

3. Navigate to the folder that you created in the previous step:

```
# cd delinea-agent/
```

4. Install the Linux Agent:

```
# ./agent_setup.sh --domain <domain name>
```



Note: There are several options you can specify if needed. For more information, display the documentation of `agent_setup.sh`:

```
# ./agent_setup.sh --help
```

5. For the UNIX computers where you have installed the Delinea agent, you need to join them to the Active Directory domain and the Privilege Control zone DelineaZone. To do this, use the `adjoin` command, either interactively at the command line or in a script. To use this command, you need to have certain privileges, and it must be run with a set of required command-line options. For details, see ["Joining Linux/UNIX Hosts to a Domain/Zone"](#) on page 636.

Installing the Windows Agent

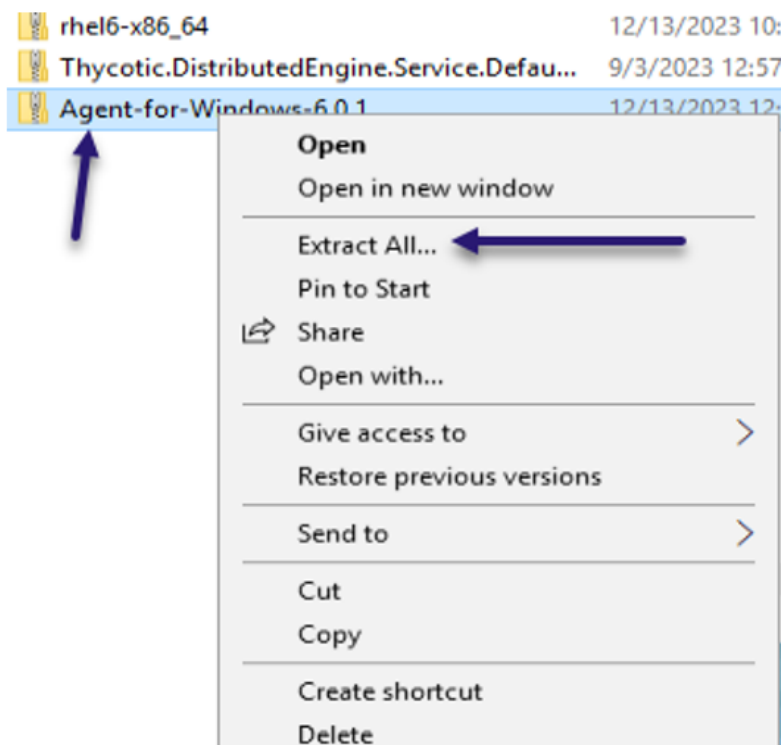
To install the Delinea Agent on a managed server that is running the Windows operating system, use the steps in this section.

Requirements:

- .Net 4.8
- Must be joined to the Active Directory domain and Privilege Control zone


Steps:

1. Log in to the server as domain administrator.
2. In the File Explorer, right-click the .zip file that you downloaded in ["Downloading the Agent"](#) on the previous page and select **Extract All...**

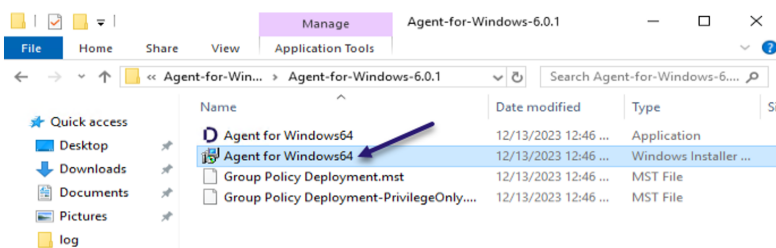


3. Click **Extract**.

When extraction is complete, the files appear in a new File Explorer window.

 **Note:** The container package is in Zip format, but the files inside are in TGZ format.

4. Open the **Agent-for-Windows-6...** folder.
5. Double-click the Windows 64 agent installer file.



6. Click **Next**. The Delinea Agent for Windows Wizard opens.
7. Click **Next**.
8. Accept the terms of the license agreement and click **Next**.
9. Keep the default destination folder and click **Next**.
10. Click **Install**.
11. Select **Run Agent Configuration Wizard**.

12. In the Agent Configuration Wizard, click **Add Service**.
13. Click **Privilege Elevation Service**, then click **OK**.
14. Select the **DelineaZone**, then click **Next**.
15. Click **Yes** to add the Domain Admins.
16. Click **Yes to Restart**.

Step 7: Scan Computer Inventory

At this point you must run Discovery to make the platform aware of your newly added computers.

1. Follow the steps at "Discovery" on page 165.
2. To be sure that Discovery found all your added machines, check the Inventory. Follow the steps at "Managing Computer Assets" on page 96.

Step 8: Set Up Authentication Profiles for PCS

Authentication profiles are required for multi-factor authentication (MFA) to function. An authentication profile specifies the authentication challenges required to log in to the platform and the length of time that must elapse before a user is prompted for authentication again.

To set up authentication profiles for PCS:

Follow the concepts and steps in "Creating Authentication Profiles" on page 473. Follow these guidelines:

- **Endpoint Login Profiles:** Authentication profiles for Endpoint Login policies should not have Challenge 1 set to Password, because the platform will always present a password challenge to the user first.
- **Local Administrator Privilege Profiles:** Profiles for Local Administrator Privilege policies should not have Challenge 1 set to Password, because the platform will always present a password challenge to the user first.
- **Emergency Access Profiles:** You do not need to create any profiles for Emergency Access policies, because their Rule Type is always Allow.

Step 9: Set Up PCS Policies

PCS authentication policies provide users with machine-level (server) permissions for logging in to remote computers and servers managed by Delinea Platform and performing actions on them. By assigning machine-level policies, you can ensure that each asset adheres to compliance standards, maintaining both security and efficiency across your network.

Follow the steps in "Setting Up PCS Policies" on page 612.

Step 10: Set Up Audit and Session Recording

To track events on Delinea Platform, you can set up audit logs and session recordings. For more details, see .

1. From the left navigation, select **Insights**, then **Session review**.
2. Log into the server as the administrator, root, or normal AD user.

To Configure on Linux:



Do not skip these steps. The Linux agent requires Direct Audit to be enabled on the Agent when policies have session recording enabled. If you skip these steps, and enable Session Recording in a Granular Privilege Elevation policy for Linux, you could be blocked from logging in to the Linux agent. See "Session Recording Stops Linux Agent Login" on page 666.

1. Log in as root user.
2. Enter the following commands:
 - `dacontrol -i DelineaPlatformAudit`
 - `dacontrol -e`
 - `dainfo`

To Configure on Windows:

1. Log in as a Domain Administrator.
2. Launch **Agent Configuration**.
3. Click **Add Service**.
4. Select **Auditing and Monitoring Service**.
5. Click **OK**.
6. On the **Enable session capture and replay** page, select **DelineaPlatformAudit**.
7. Click **Next**.

Audit and Monitoring configuration is complete.

Viewing Audit Session Recordings

From the left navigation, select **Insights**, then **Session review**.

Log in to the Linux and Windows servers as the administrator, root, or a normal AD user.

Linux

When logging in to a Linux server, use one of the following options:

- Run commands as root user.
- Run commands as a normal AD user. Elevate commands as a normal AD user having the Local Administrator Privileges policy using the `dzdo` command.

Windows

When logging in to a Windows server, use one of the following options:

- Run programs as the administrator.
- Run commands as a normal AD user. Launch elevated desktop as a normal AD user having the Local Administrator Privileges policy.

Step 11: Set Up Use My Account

You can set up Use My Account (UMA) so you can access enrolled Linux systems without an additional login step. UMA provides single sign-on to Linux systems for users who are logged in to the Delinea Platform.

See "Setting Up Use My Account" on page 621.

Supported Operating Systems for Agents

The following operating systems are supported for the Delinea Agent.

For an overview of PCS and its components, see "Setting Up PCS" on page 601.

Supported UNIX/Linux Platforms

Supported Platforms	CPU	Express	DirectControl	DirectAudit	Remark
AlmaLinux 8.5-8.10, 9.0-9.4	x86_64	Yes	Yes	Yes	
Alpine Linux 3.17-3.20	X86_64	No	Yes	Yes	
Amazon Linux 2 LTS	aarch64	No	Yes	Yes	
Amazon Linux 2 LTS	x86_64	No	Yes	Yes	
Amazon Linux 2023	x86_64	No	Yes	Yes	
CentOS 7.4-7.9	aarch64	No	Yes	Yes	
CentOS 7.0-7.9	x86_64	Yes	Yes	Yes	
Debian 10.0-10.11, 11.0-11.7, 12.0-12.9	x86_64	Yes	Yes	Yes	
Flatcar	x86_64	No	Yes	Yes	
HP-UX 11.31 (Trusted and Untrusted)	Itanium	No	Yes	Yes	
IBM AIX 7.2, 7.3	ppc	No	Yes	Yes	Note 3
IBM Virtual I/O Server 3.x	ppc	No	Yes	Yes	
Oracle Linux 7.4-7.9, 8.0-8.10, 9.0-9.4	aarch64	No	Yes	Yes	
Oracle Linux 7.0-7.9, 8.0-8.10, 9.0-9.4	x86_64	Yes	Yes	Yes	

Supported Platforms	CPU	Express	DirectControl	DirectAudit	Remark
Oracle Solaris 10 u8+, 11.3-11.4	SPARC	No	Yes	Yes	Note 2
Oracle Solaris 10 u8+, 11.3-11.4	x86_64	No	Yes	Yes	Note 2
Red Hat Enterprise Linux 8.0-8.10, 9.0-9.4	aarch64	No	Yes	Yes	
Red Hat Enterprise Linux 7.0-7.9	ppc64	Yes	Yes	Yes	
Red Hat Enterprise Linux 7.1-7.9, 8.0-8.10, 9.0-9.4	ppc64le	Yes	Yes	Yes	
Red Hat Enterprise Linux 7.0-7.9, 8.0-8.10, 9.0-9.4	x86_64	Yes	Yes	Yes	
Fedora Linux 39, 40	x86_64	Yes	Yes	Yes	
Rocky Linux 8.5-8.10, 9.0-9.4	x86_64	Yes	Yes	Yes	
SUSE Linux Enterprise 12 SP3+, 15	aarch64	No	Yes	Yes	
SUSE Linux Enterprise 12 SP3+, 15	ppc64le	Yes	Yes	Yes	
SUSE Linux Enterprise 12 SP3+, 15	x86_64	Yes	Yes	Yes	
Ubuntu Linux 20.04, 22.04, 23.10, 24.04	arm64	No	Yes	Yes	
Ubuntu Linux 20.04, 22.04, 23.10, 24.04	ppc64el	No	Yes	Yes	
Ubuntu Linux 20.04, 22.04, 23.10, 24.04	x86_64	Yes	Yes	Yes	

Note 1: OS patch level update 8 or above on Solaris 10 is required.

Note 2: TL1 or above on AIX 7.1 is required.

Note 3: Smart Card doesn't work on Ubuntu Linux 24.04 due to a GNOME bug ([#7562](#)).

Additional Information

You should follow the OS vendors' recommendation to update the necessary patches. The minimum patch requirements for the specific UNIX platforms are as follows (CS-45562):

1. HPUX 11.31
 - a. PHNE_40225 - Cumulative Console and BSD Pty Patch (it is required for DirectAudit package)

2. Solaris 10 x86_64

- a. 119255-66
- b. 127128-11
- c. 141445-09
- d. 142910-17

3. Solaris 10 SPARC

- a. 119254-66
- b. 120011-14
- c. 127127-11
- d. 142909-17

Supported Windows Platforms

The following 64-bit Windows platforms are supported:

- Windows 10 LTSC/LTSC (Note 1)
- Windows 11 LTSC/LTSC
- Windows Server 2016
- Windows Server 2019 LTSC
- Windows Server 2022 LTSC
- Windows Server 2025

We support Windows 10 Long Term Servicing Channel (LTSC), or previously called Long Term Servicing Branch (LTSB), editions based on Microsoft's lifecycle factsheet; see <https://docs.microsoft.com/en-us/lifecycle/faq/windows> and <https://docs.microsoft.com/en-us/windows/release-health/release-information>.

Setting Up PCS Policies

PCS authentication policies provide users with machine-level (server) permissions for logging in to remote computers and servers managed by Delinea Platform and performing actions on them. By assigning machine-level policies, you can ensure that each asset adheres to compliance standards, maintaining both security and efficiency across your network.

For a policy to grant access, all the policy's rules and conditions must be satisfied, and the user must not be denied access by a different policy with the same rules and conditions.

Viewing Policies

From the left navigation, select **Policies**. The Policies page opens, listing each policy available in your platform environment on a table row, with columns for details including the policy name, state, deployment status, and policy type.

Deployment Status

Deployment Status refers to the deployment of the policy on the target. The status can be Active, Activating, Active - incomplete, Activation Failed, Deactivating, Deactivation Failed, or Inactive. The Activating and Deactivating statuses appear for just a few seconds.

When the policy is not being enforced on one or more targets that are included in the policy, because the Delinea Agent is not installed on the targets, a warning message is displayed in the Deployment Status area. Click the message to get a list of the affected computers.

Creating a Policy

To define a policy, use the following steps.

1. From the left navigation, select **Policies**. The Policies page opens, listing each policy available in your platform environment.
2. Click **Create Policy**.
3. On the Create Policy page, click a radio button to select a policy type from among the types listed. A policy type is defined by the events you want to control. Select one of the following:

- **Emergency Access:** Users who meet the conditions defined in this policy can log in and perform elevation actions when a server can not communicate with the Delinea Platform.



We strongly suggest that you define and enable an Emergency Access policy, at the minimum, to avoid losing access to your Delinea Platform instance.

- **Endpoint Login:** Users who meet the conditions defined in this policy can log in to any computer where the policy is enabled.
- **Local Administrator Privileges:** Users who meet the conditions defined in this policy gain administrative privileges on the target agent. The user can run any command as administrator or root. On Windows, the Run with Privilege option is used; on Linux, the dzdo command is used.

- **Granular Privilege Elevation:**

For users who meet the conditions defined in this policy, administrators can assign elevated permissions so they can run commands on Windows and Unix/Linux servers.

In a standard UNIX shell environment, an ordinary user account can execute a large number of common command-line programs without any special privileges, but one or more administrative accounts, such as root, are required to execute commands that perform privileged operations. If ordinary users need to execute any of the commands requiring administrative privileges, they might have to switch to an administrative account that requires them to know the password for a privileged user, or they might be granted access by configuration settings in a sudoers file. A Granular Privilege Elevation policy makes it easier to grant this sort of access. You can grant certain users permission to execute commands that would otherwise require administrative or root privileges.

4. Click **Select template**. A page opens where you can create a new policy. For details about how to fill out this page, see the next few sections.

Policy Details

In the first section of the Create Policy page, specify the basic information about the policy.

1. Enter a policy name in the **Name** field.
2. (Optional) Enter a policy description in the **Description** field.
3. Select the box next to Enabled to enable the policy.

Command Groups

(For Granular Privilege Elevation policies only)

A Granular Privilege Elevation policy controls access on Delinea Platform managed computers to all the commands in the command group. In this section of the Create Policy page, choose one or more command groups to specify which commands you want to enable users to run.

Each command group contains a set of command-line programs. Before you can add command groups to a policy, you must first define the commands, then add them to command groups, as described in the next few sections.

Creating Commands

If needed, create one or more new commands. Commands are configured by defining command rights, adding the rights to the appropriate roles, and assigning the roles to different users and groups. Users who have been assigned the appropriate roles can then run privileged commands by invoking the `dzdo` command.

The most common reason for defining a command right is to grant access to commands that perform privileged operations. For example, you might want to grant users additional privileges to execute specific commands in a standard shell environment that they are not otherwise allowed to execute with the default rights associated with their account.

You can define command access rights to tightly control the specific commands users can execute. You can also refine those rights to only allow specific arguments to be used or to require an executable to be located in a specific directory.

1. From the left navigation, select **Policies**, then **Commands**.
2. Click **Create command** and choose the operating system: Linux/Unix or Windows.
3. Click **Create custom command**.
4. Enter a name and (optional) description.

The name is required and must not be more than 63 characters in length or contain any special characters, such as asterisks (*), slashes (/), question marks (?), or quotation marks (").

The rest of the steps depend on whether you are defining a Linux/Unix command or a Windows command.

- For a Linux/Unix command, use steps 5 - 8.
- For a Windows command, use steps 9 - 12.

5. (Linux/Unix) In **Command**, give the name of the command as you would enter it at the command line; for example, `vi`.

You can also use wild cards or a regular expression to specify commands matching a particular pattern.

6. (Linux/Unix) In **Arguments**, give any input arguments that the command requires; for example, `/etc/ssh/sshd_config` to edit the SSH server's config file. Glob pattern matching is used to expand any wildcard expressions. If you do not specify any arguments, the default value of asterisk (*) is used.
7. (Linux/Unix) In **Match path**, choose the path where the command can be found:
 - Select **Standard user path** to use the local operating system's common set of user directories to find the command; for example, `/bin`, `/usr/bin`.
 - Select **Standard system path** to use the directories the root user would normally get on the local operating environment to find the command; for example, `/sbin`, `/usr/sbin`
 - Select **System search path** to search for the command in a predefined set of locations. The search locations are defined using the `dzdo.search_path` configuration parameter. If you select System search path and the `dzdo.search_path` parameter is not defined, the current user's path is used to search for the command. For example, `/sbin`, `/usr/sbin`, `/bin`, `/usr/bin`.
 - Select **Specific path** to define a custom set of locations for finding the command specified. You can specify one or more paths, separated by a colon. If you set both **Command** and **Specific path** to match all strings (*), any command from any path is allowed.
8. (Linux/Unix) In **Run command as**, choose the user role that determines the permissions that will be used to run the command. You can specify a user account or run the command as root. The user account must be present on the endpoint.

In most cases, the local root account is the appropriate account to use, because it allows ordinary users to execute the specified command using root account privileges. However, you can click **Add** to add other users, groups, or service accounts that can be used to execute the command. Use the format `#UID` for UID values, `%group` for group names, or `%#GID` for GID values.

The account used to execute commands can be an Active Directory user with a UNIX profile in the zone or a local UNIX user account. However, the account used to log on and invoke the command using `dzdo` must be associated with an Active Directory account.



The role that is set in **Run Command As** is only applicable to users executing policies under the `dzdo` command. Users with the Restricted Shell (`dzsh` defined as their login shell) continue to execute policies as the logged-in user.

9. (Windows) In **Application**, give the name of the application runtime file; for example, `taskschd.msc`.
10. (Windows) In **Arguments**, give any input arguments that the application requires; for example, `\s`. If you do not specify any arguments, the field is left blank.



Note: The use of the asterisk (*) as an argument is not supported. The value `/*` can be used as an argument, but it does not act as a wildcard. The literal text `/*` is used.

11. (Windows) In **Match path**, choose the path where the command can be found:
 - Standard system path
 - Specific path; for example, `%systemroot%\system32\`

12. (Windows) In **Run command as**, select one of the following to choose the user or group whose permissions will be used to run the command:
 - To use a Windows built-in security group: Choose **Built-in group** from the dropdown, then choose one of the provided Active Directory security groups. For more information about these groups, see [Active Directory security groups](#) in the Microsoft documentation.
 - To use an individual user: Choose **AD domain user** from the dropdown, then click **Select a domain user** to search for and select a user account. The user account must be present on the endpoint.
 - To use an Active Directory security group that is defined in one of the domains accessible to your policy: Choose **AD domain group** from the dropdown, then click **Select a domain group** to search for and select an Active Directory domain group.
13. Click **Create command**.

The command is saved, and the Commands list page is displayed again. The new command appears in the list.

If needed, repeat these steps to create more commands.

Creating Command Groups

After creating all the commands you need, create command groups.

1. From the left navigation, select **Policies**, then **Command groups**.
2. Click **Create command group**.
3. Enter a name and (optional) description.
4. Click **Assign command**.
5. Click one or more checkboxes next to the commands you want to include in the command group.

If you are not sure which commands to choose, you can click the name of any command to see its details.
6. Click **Create group**.

If needed, repeat these steps to create more command groups.

Adding Command Groups to the Policy

After creating all the command groups you need, you are ready to fill out the Command Groups part of the Create Policy page for a Granular Privilege Elevation policy.

1. Click **Add command groups**.

The Select Command Groups page shows all the command groups that have been defined.
2. Click one or more checkboxes next to the command groups you want to include in the policy.

If you are not sure which groups to choose, you can click the name of any group to see which commands it includes.

Modifying Commands and Command Groups

You can edit commands and command groups after creating them and adding them to policies. To do so, display the command or command group and click **Edit** or **Delete**.

Privilege Control for Servers

The Delinea Platform keeps track of changes to commands and command groups. The platform records the modification date and the username of the person who made the change. The platform then updates its display wherever the changed entity is shown.

For example, when a command is modified, the modification date and username are updated and displayed in the following pages:

- Commands page, which lists all of the commands
- Pages for any command group that contains the command
- Pages for any policy that includes a command group where the command is a member

When a command is added to a command group or removed from a command group, the date and username are updated and displayed in the following pages:

- Command Groups page, which lists all the command groups
- Pages for any policy that includes the command group

When a command is deleted, the date and username are updated and displayed in the following pages:

- Pages for any command group that contained the command
- Pages for any policy that included a command group where the command was a member

When a command group is deleted, the date and username are updated and displayed in the pages for any policy that included the command group.

Policy Subjects

After filling out the Policy Details section, choose the policy subjects. Subjects are the users and user groups your policy can apply to, based on the template you selected earlier.

1. Scroll down to the **Subjects** section to see a list of available subjects.
2. Click the **Add Subjects** button.
3. Select the box next to each AD user and user group you wish to add to the policy.
4. Click the **Update** button.

Policy Targets

Targets are the computers and computer groups your policy can apply to. The target is where the Subject can perform an action, based on the template you selected earlier.

1. Scroll down to the **Targets** section.

To define the targets, make one of the following choices:

- To add individual computers and computer groups, click **Add computers**. In the Select Computers dialog, select the box next to each computer and computer group your policy will apply to.

Computers where the Delinea Agent is installed and AD computers where the Delinea Agent is not yet installed can all be selected as policy targets. To see whether a computer has the agent installed, see ["Checking for Agent Installation" on page 605](#).

- To add collections, click **Add collections**. In the Select Collections dialog, select the box next to one or more collections, then click **Add Collections**. For more information about collections, see [Grouping with Computer Collections](#).

2. Click the **Update** button.

When you finish defining the policy and you set its status to Enabled, the policy will start to be enforced on the selected targets where the Delinea Agent is installed.

For any target that does not have the Delinea agent installed, a policy that is set to Enabled will start to be enforced whenever the agent is installed and the target is joined to a domain and zone. A message is displayed on the Policy page to let you know when one or more targets that are included in the policy are not being enforced because the agent is not installed. Click the message to get a list of these computers so you can remedy the situation. You can download the list in CSV format.

For more information about installing the agent or determining whether it is already installed on a computer, see ["Step 6: Install the Delinea Agent on Managed Servers" on page 604](#) in the PCS Setup page.

Policy Conditions

(Optional) Conditions define when or how the policy should be applied. If a policy has a time range condition, the policy will apply only within that time range. All of the time conditions must be met. Local time, not universal time, is used.

If a policy has no time range condition, the policy will apply at all times.

1. Scroll down to the **Conditions** section.
2. Click **Add Condition**.
3. In **Condition Type**, click inside the *Search or pick one* box.
4. Select one of the condition types displayed or enter text to search.

When you have selected a condition type, options appear below **Constraint**.

5. Set the constraints for the condition you selected.
6. To add another condition, click **Add Condition** again and follow the same procedure.

Policy Controls


Controls are additional requirements the user must meet to fulfill the requirements of the policy. All of the control conditions must be met.

Policy controls can be set in the following ways:

- **MFA**: Requires multi-factor authentication. If you select MFA, a new *Search or pick one* box appears. Select an Authentication Profile to specify which MFA challenges the user must pass and how much time will elapse before the user is prompted again for authentication. Emergency Access profiles always allow access without MFA, so the option is not shown.

- **Require Session Recording:** Denies access if session recording cannot be performed on the endpoint. For example, session recording is not available if the audit service is not enabled on the endpoint or a session recording process is blocked. Require Session Recording can be assigned as the only control, or in conjunction with MFA. Require Session Recording can be also be applied to local administrator privileges. Emergency Access profiles always allow access without session recording, so the option is not shown.

To define policy controls:

1. Scroll down to the **Controls** section.
 2. Select **MFA** if you want to require multi-factor authentication.
Emergency Access profiles always allow access without MFA, so the option is not shown.
 3. If you selected MFA, a dropdown list box appears. Select an authentication profile.
 4. In **Session Recording**, select one or both of the following:
 - **Audit enabled:** Select this option to record the user's activity.
 - **Required:** Select this option if you want to deny user access when session recording can not be performed. **Audit enabled** must also be selected. If the **Required** option is not selected, but **Audit enabled** is, the user's activity is audited if possible, but user access is not denied if auditing is not possible.
-  **Note:** Emergency Access profiles always allow access without session recording, so the **Required** option is not shown.
5. When you have made all the required changes, click **Create Policy**.
 6. Click **Activate** to activate the policy.

Enabling IWA on the Default Identity Policy

For PCS to function, IWA must be enabled on the default identity policy.

1. From the left navigation, select **Access**, then **Identity policies**.
2. Click to open the **Default Policy**.

Identity Policies

Manage access policies for platform members. Policies can be arranged in order of priority with the highest priority at the top.

Reorder

Add Policy

Q Search

4 items



	NAME	STATUS	DESCRIPTION
1	fsadfsadf	Active	fdsfsdf
2	example-local	Active	
3	PM-XPM-Domain-Portal-Login	Active	
4	Default Policy	Active	Default Policy Settings.

3. Select the **Authentication** tab.
4. Scroll to the Other Settings section and click **Edit**.

Other Settings

IWA connections

- ☒ Allow IWA connections (bypasses authentication rules and default profile)
 - ☒ Set identity cookie for IWA connections
 - ☒ IWA connections satisfy all MFA mechanisms

Other

- ☒ Allow users without a valid authentication factor to log in
- ☐ Connections via federation satisfy all MFA mechanisms
- ☒ Allow additional authentication from same device
- ☐ Continue with additional challenges after failed challenge
 - ☐ Do not send challenge request when previous challenge response failed
- ☐ Remember and suggest last used authentication factor

Cancel

Save

5. Enable IWA connections and the two available IWA options.
6. Click **Save**.
7. Log in to the Delinea Platform as one of the AD users you created.

Setting Up Use My Account

You can set up Use My Account (UMA) so you can access enrolled Linux/UNIX computers without an additional login step. UMA provides single sign-on to Linux computers for users who are logged in to the Delinea Platform.

This section describes several different ways to set up Use My Account for *nix computers.

Using Delinea OpenSSH

To automatically set up UMA for *nix systems, run the `agent_setup.sh` script during the agent installation.

Using OS Stock Version of OpenSSH

The `agent_setup.sh` script automatically sets up UMA during the agent installation process.

Using Automatic Script for UMA

1. Navigate to where you downloaded the agent from the Delinea Marketplace.
2. Run the following script with root permissions:

```
./uma_setup.sh --install-cakey-file delinea_<tenantname>_date.pub -v
```

Example:

```
./uma_setup.sh --install-cakey-file delinea_jwtraining-us_20240125_124856.pub -v
```

```
[root@lin-svr-01 agent]# ll
total 121164
-r-xr-xr-x. 1 root root 12392232 Dec 12 13:12 adcheck-rhel6-x86_64
-rwxr-xr-x. 1 root root 8522 Jan 25 12:48 adclient_deploy.sh
-rwxr-xr-x. 1 root root 5907 Jan 25 12:48 agent_setup.sh
-r--r--r--. 1 root root 6608572 Oct 14 08:10 CentrifyDA-6.0.1-320-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 37 Dec 12 18:36 CentrifyDA-6.0.1-rhel6.x86_64.rpm -> CentrifyDA-6.0.1-320-rhel6.x86_64.rpm
-r--r--r--. 1 root root 18665100 Dec 12 13:43 CentrifyDC-6.0.1-376-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 37 Dec 12 18:36 CentrifyDC-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-6.0.1-376-rhel6.x86_64.rpm
-r--r--r--. 1 root root 13484 Dec 12 13:44 CentrifyDC-cifsmap-6.0.1-376-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 47 Dec 12 18:36 CentrifyDC-cifsmap-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-cifsmap-6.0.1-376-rhel6.x86_64.rpm
-r--r--r--. 1 root root 406068 Dec 12 13:43 CentrifyDC-curl-6.0.1-376-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 42 Dec 12 18:36 CentrifyDC-curl-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-curl-6.0.1-376-rhel6.x86_64.rpm
-rw-rw-r--. 1 root root 1394 Feb 22 2023 centrifydc-install.cfg
-r--r--r--. 1 root root 792376 Dec 12 13:44 CentrifyDC-ldapproxy-6.0.1-376-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 47 Dec 12 18:36 CentrifyDC-ldapproxy-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-ldapproxy-6.0.1-376-rhel6.x86_64.rpm
-r--r--r--. 1 root root 225752 Dec 12 13:44 CentrifyDC-nis-6.0.1-376-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 41 Dec 12 18:36 CentrifyDC-nis-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-nis-6.0.1-376-rhel6.x86_64.rpm
-r--r--r--. 1 root root 597380 Dec 12 13:43 CentrifyDC-openldap-6.0.1-376-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 46 Dec 12 18:36 CentrifyDC-openldap-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-openldap-6.0.1-376-rhel6.x86_64.rpm
-r--r--r--. 1 root root 1436992 Oct 5 12:05 CentrifyDC-openssh-9.3p1-6.0.1-370-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 51 Dec 12 18:36 CentrifyDC-openssh-9.3p1-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-openssh-9.3p1-6.0.1-370-rhel6.x86_64.rpm
-r--r--r--. 1 root root 4917224 Dec 12 13:43 CentrifyDC-openssl-6.0.1-376-rhel6.x86_64.rpm
lrwxrwxrwx. 1 root root 45 Dec 12 18:36 CentrifyDC-openssl-6.0.1-rhel6.x86_64.rpm -> CentrifyDC-openssl-6.0.1-376-rhel6.x86_64.rpm
-rw-rw-r--. 1 root root 57624 Feb 22 2023 centrify-suite.cfg
-rwxr-xr-x. 1 root root 92 Jan 25 12:48 delinea_jwtraining-us_20240125_124856.pub
-rwxr-xr-x. 1 root root 38730588 Jan 25 12:48 delinea-server-suite-2023.1-rhel6-x86_64.tgz
lrwxrwxrwx. 1 root root 10 Oct 12 14:09 install-express.sh -> install.sh
-r-xr-xr--. 1 root root 416446 Oct 12 14:09 install.sh
-rwxr-xr-x. 1 root root 1082 Jan 25 12:48 readme.txt
-rw-r--r--. 1 root root 38729195 Jan 25 07:49 rhel6-x86_64.zip
-rwxr-xr-x. 1 root root 17710 Jan 25 12:48 uma_setup.sh
[root@lin-svr-01 agent]# ./uma_setup.sh --install-cakey-file delinea_jwtraining-us_20240125_124856.pub -v
Need to install new CA key(s)
Remove old CA key: ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIJ2feixLiZEil+ldlmLBUcu770edDl0aJ99fFo0McZbO Default CA
Old CA key(s) removed
New CA key(s) installed
sshd config updated
sshd restarted
[root@lin-svr-01 agent]#
```

Using Manual Steps

1. Navigate to and open the folder where you downloaded the agent from the Delinea Marketplace.

The agent is a .pub file in the following format:

delinea_{tenant-name}_{download-date}.pub

2. Copy the .pub file to the ssh directory.

Example:

```
cp delinea_{tenant-name}_{download-date}.pub /etc/ssh/users_ca.pub
```

```
cp delinea_fishing_20231213_041058.pub /etc/ssh/users_ca.pub
```

3. Make a backup copy of the sshd_config file:

```
cp /etc/ssh/sshd_config /etc/ssh/sshd_config_121323bk
```

4. Edit the sshd_config file with the following lines:

- Example command: vi /etc/ssh/sshd_config
- AuthorizedPrincipalsCommand /usr/bin/adquery user -P %u
- AuthorizedPrincipalsCommandUser root
- TrustedUserCAKeys /etc/ssh/users_ca.pub

```
#versionaddendum none
# no default banner path
#Banner none

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
Subsystem sftp /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#    X11Forwarding no
#    AllowTcpForwarding no
#    PermitTTY no
#    ForceCommand cvs server
AuthorizedPrincipalsCommand /usr/bin/adquery user -P %u
AuthorizedPrincipalsCommandUser root
TrustedUserCAKeys /etc/ssh/users_ca.pub
```

5. Restart OpenSSH Service.

Example:

```
systemctl restart sshd.service
```

```
[root@lin-svr-01 delinea-agent]# systemctl restart sshd.service
[root@lin-svr-01 delinea-agent]# systemctl status sshd.service
sshd.service - OpenSSH server daemon
Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor preset: enabled)
Active: active (running) since Wed 2023-12-13 14:33:56 EST; 7s ago
Docs: man:sshd(8)
      man:sshd_config(5)
Main PID: 248879 (sshd)
Tasks: 1 (limit: 11144)
Memory: 1.2M
CGroup: /system.slice/sshd.service
        └─248879 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20-poly1305@openssh.com

Dec 13 14:33:56 lin-svr-01.delinea-se.lab systemd[1]: sshd.service: Succeeded.
Dec 13 14:33:56 lin-svr-01.delinea-se.lab systemd[1]: Stopped OpenSSH server daemon.
Dec 13 14:33:56 lin-svr-01.delinea-se.lab systemd[1]: Starting OpenSSH server daemon...
Dec 13 14:33:56 lin-svr-01.delinea-se.lab sshd[248879]: Server listening on 0.0.0.0 port 22.
Dec 13 14:33:56 lin-svr-01.delinea-se.lab sshd[248879]: Server listening on :: port 22.
Dec 13 14:33:56 lin-svr-01.delinea-se.lab systemd[1]: Started OpenSSH server daemon.
```

Test Use My Account






 **Note:** UMA is only for *nix systems with the agent installed that is joined to the domain and zone.

1. Log in to the platform as an AD user with permission to log in to the Linux system.
2. From the left navigation, select **Inventory**.
3. Find and the server with the agent installed that is joined to the domain and zone.
4. Hover your cursor over the row with the target computer, and click the launch icon.

Assets Preview

Manage Computers from this centralized location. [Learn more](#)

5 items

COMPUTER NAME ↑	TYPE	DOMAIN	OPERATING SYSTEM	CLIENT VERSION	CREATED DATE	LAST MODIFIED
 DC-2022	Server	pm-xpm.local	Windows	6.0.1-362	09/20/2023 10:43 am	01/20/2024 04:56 pm
 ENGINE-2022-2	Server	pm-xpm.local	Windows	6.0.1-362	01/18/2024 11:39 am	01/20/2024 04:56 pm
 LIN-SVR-01	Server	pm-xpm.local	Linux	CentrifyDC 6.0.1-375	09/20/2023 10:43 am	01/18/2024 12:32 pm
 RAS-LINUX	Server	pm-xpm.local	Linux	CentrifyDC 6.0.1-375	09/20/2023 10:43 am	01/18/2024 12:32 pm
 WIN-SVR-01	Server	pm-xpm.local	Windows	6.0.1-360	09/20/2023 10:43 am	01/18/2024 01:39 pm

5. Select **Launch with My Account**.

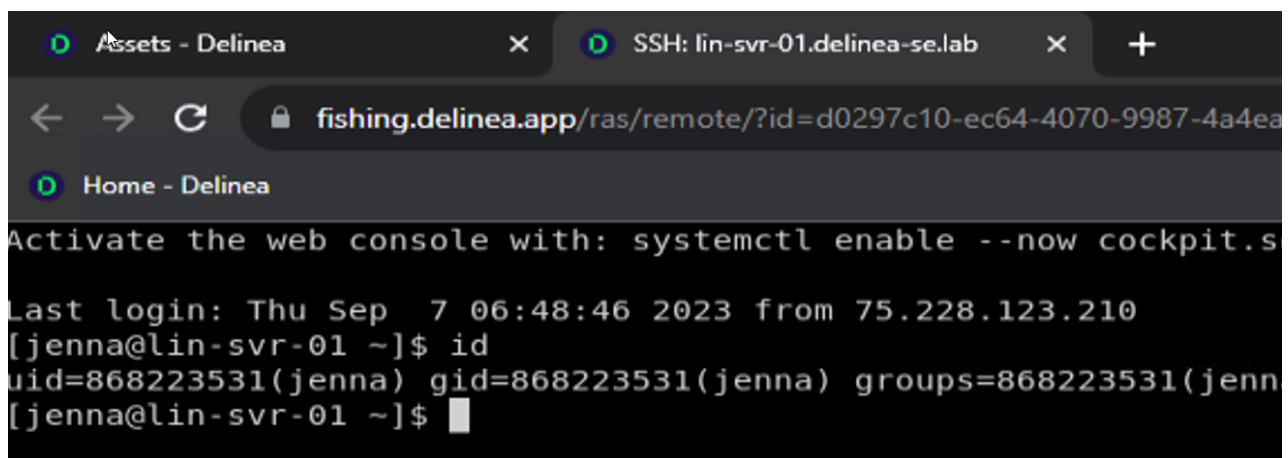
Launch Remote Session

 Launch with Manual Credential

 Launch with My Account

 Launch with Secret

Cancel

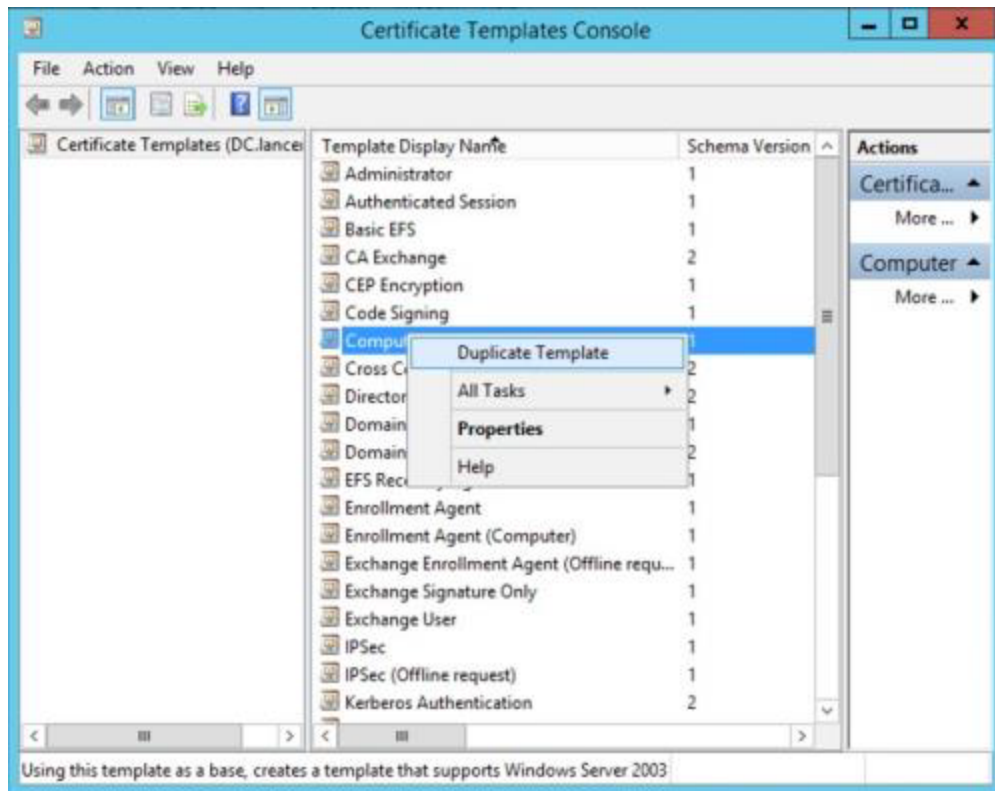


Setting Up a Certificate for Internal MS CA

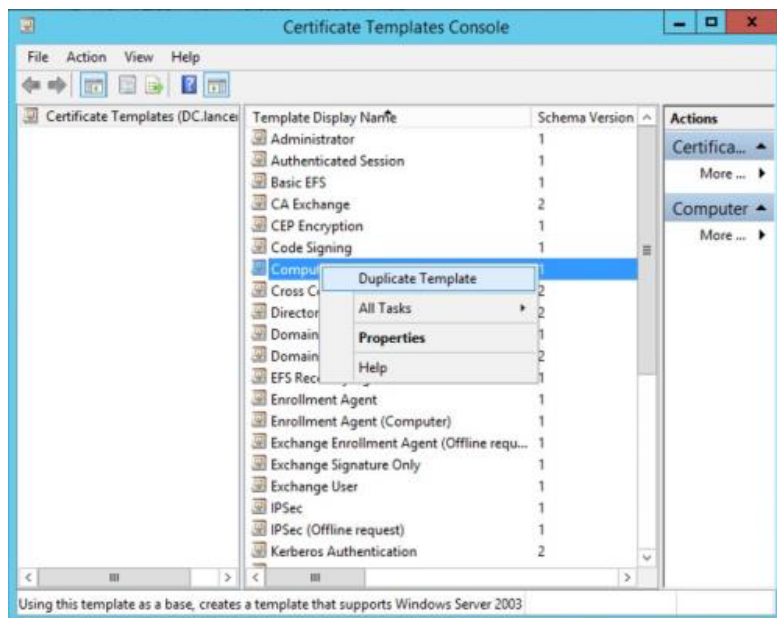
This section describes how to create a machine certificate for use with a connector for Privilege Control for Servers. The connector requires a signed certificate and root of trust in order to communicate with the Delinea Platform. You install the certificate onto the computer where you have installed the Delinea Connector.

To create a computer certificate template with an exportable private key

1. In your domain's Certification Authority (CA), open the **Certification Authority** program and expand the CA.
2. Right-click **Certificate Templates** and select **Manage**. This opens the **Certificate Templates** console.



3. Scroll down, right click the **Computer** template, and select **Duplicate Template**. This opens the new certificate template window.



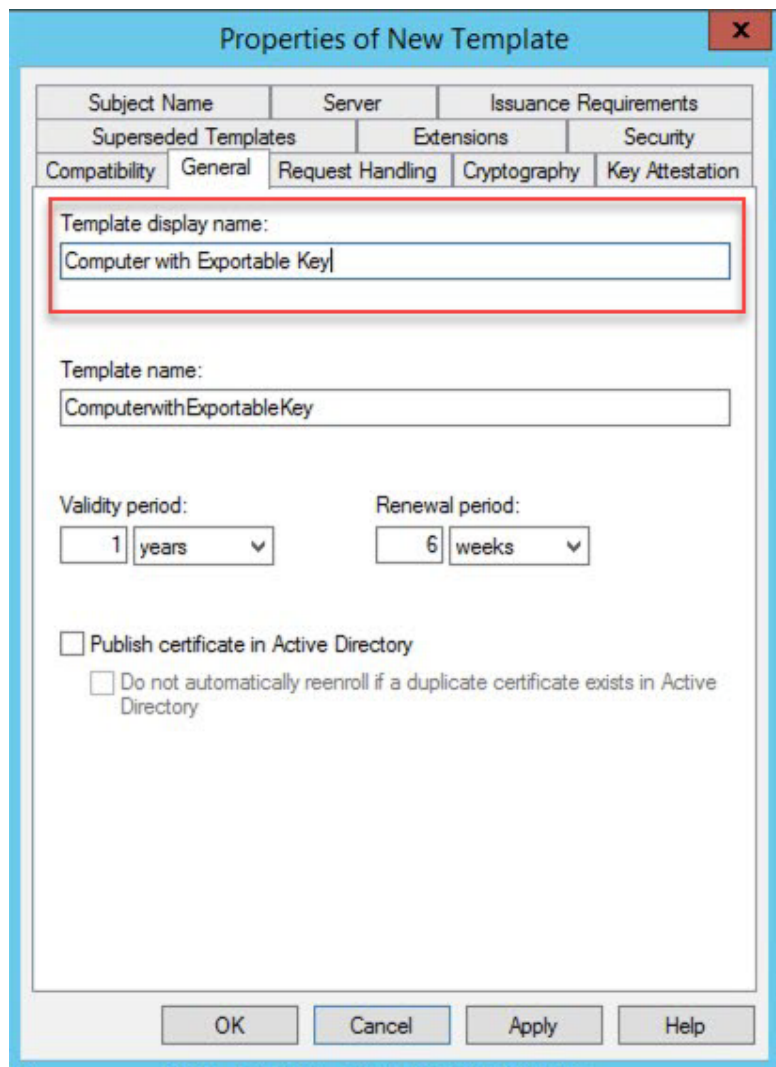
4. Select the **Compatibility Settings** tab.

- For the **Certification Authority** field, select **Windows Server 2012 R2** or higher.
- For the **Certificate Recipient** fields, select **Windows 8.1 Windows Server 2012 R2** or higher.



The image shows a 'Compatibility Settings' dialog box. It has two dropdown menus. The first is labeled 'Certification Authority' and is set to 'Windows Server 2012 R2'. The second is labeled 'Certificate recipient' and is set to 'Windows 8.1 / Windows Server 2012 R2'.

5. Select the **General** tab. In **Template display name**, enter Computer with Exportable Key.



The image shows the 'Properties of New Template' dialog box. The 'General' tab is selected. The 'Template display name' field is highlighted with a red box and contains the text 'Computer with Exportable Key'. The 'Template name' field contains 'ComputerwithExportableKey'. The 'Validity period' is set to '1 years' and the 'Renewal period' is set to '6 weeks'. There are checkboxes for 'Publish certificate in Active Directory' and 'Do not automatically reenroll if a duplicate certificate exists in Active Directory', both of which are currently unchecked. At the bottom are buttons for 'OK', 'Cancel', 'Apply', and 'Help'.

6. Select the **Request Handling** tab and select **Allow the private key to be exported**.

Properties of New Template

Subject Name	Server	Issuance Requirements
Superseded Templates	Extensions	Security
Compatibility	General	Request Handling
		Cryptography
		Key Attestation

Purpose: Signature and encryption

☐ Delete revoked or expired certificates (do not archive)

☐ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

☐ Authorize additional service accounts to access the private key

Key Permissions...

☒ Allow private key to be exported

☐ Renew with the same key

☐ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

☒ Enroll subject without requiring any user input

☐ Prompt the user during enrollment

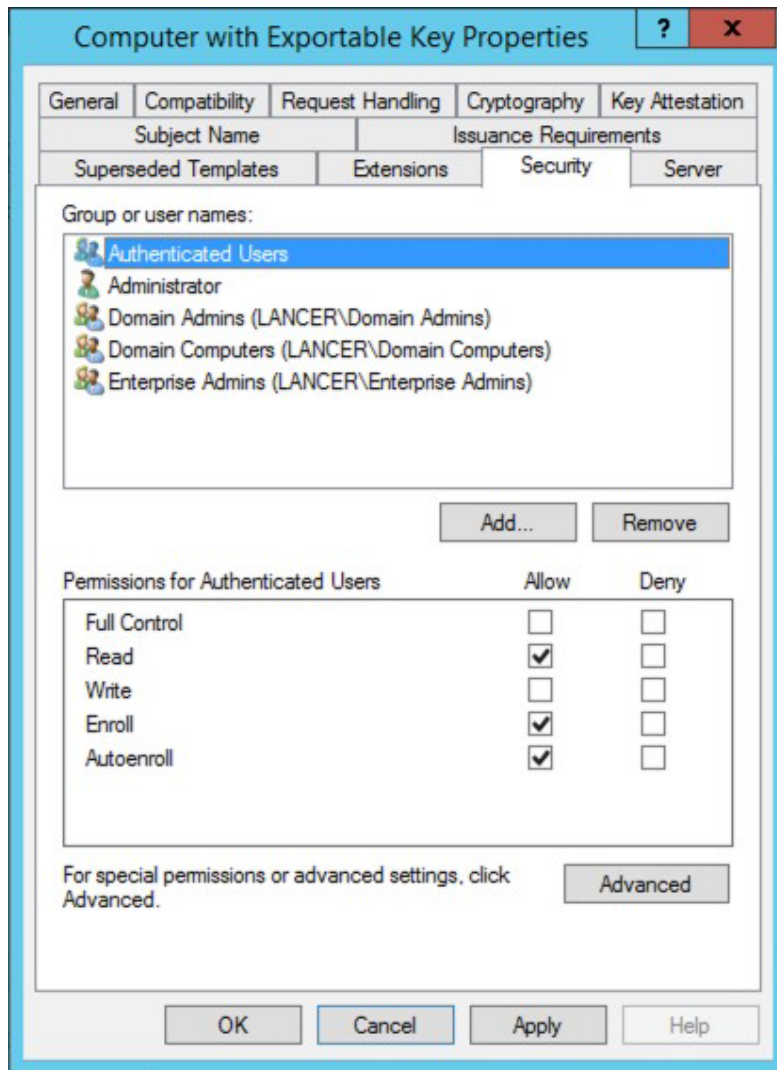
☐ Prompt the user during enrollment and require user input when the private key is used

OK Cancel Apply Help

7. Select the **Subject Name** tab and choose **Supply in the Request**.

The screenshot shows a Windows-style dialog box titled "Computer with Exportable Key Properties". It has a standard title bar with a question mark and a close button. The dialog contains several tabs: "General", "Compatibility", "Request Handling", "Cryptography", "Key Attestation", "Superseded Templates", "Extensions", "Security", and "Server". The "Security" tab is currently selected. Inside the "Security" tab, there are two sub-sections: "Subject Name" and "Issuance Requirements". Under "Subject Name", there are two radio buttons. The first is "Supply in the request", which is selected. Below it is a checkbox "Use subject information from existing certificates for autoenrollment renewal requests", which is unchecked. The second radio button is "Build from this Active Directory information", which is also unchecked. Below this is a text box "Select this option to enforce consistency among subject names and to simplify certificate administration." followed by a label "Subject name format:" and a dropdown menu currently showing "None". Below the dropdown is a checkbox "Include e-mail name in subject name", which is unchecked. Under the heading "Include this information in alternate subject name:", there are four checkboxes: "E-mail name", "DNS name", "User principal name (UPN)", and "Service principal name (SPN)", all of which are unchecked. At the bottom of the dialog are four buttons: "OK", "Cancel", "Apply", and "Help".

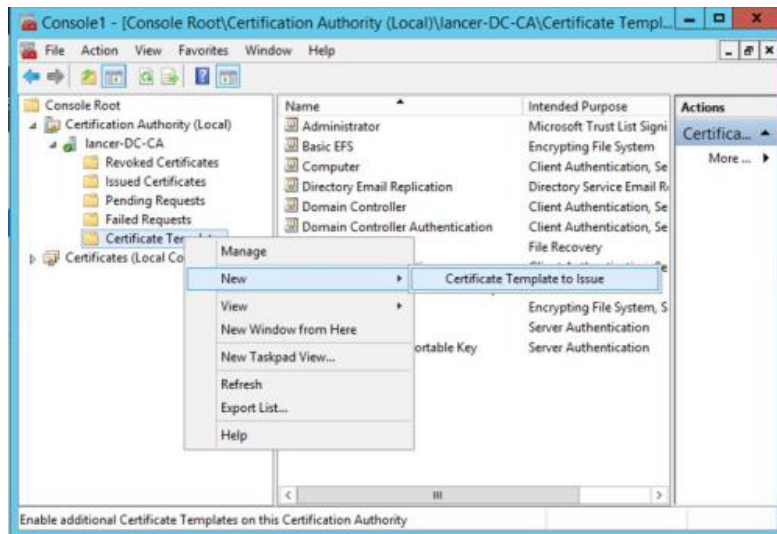
8. Select the **Security** tab. Authenticated users are highlighted. In the lower pane, select **Enroll** and **AutoEnroll**.



9. Click **OK**.
10. In the **Certification Authority** console, right-click **Certificate Templates** and select **New > Certificate Templates to Issue**.

The **Enable Certificate Templates** window opens.

Privilege Control for Servers



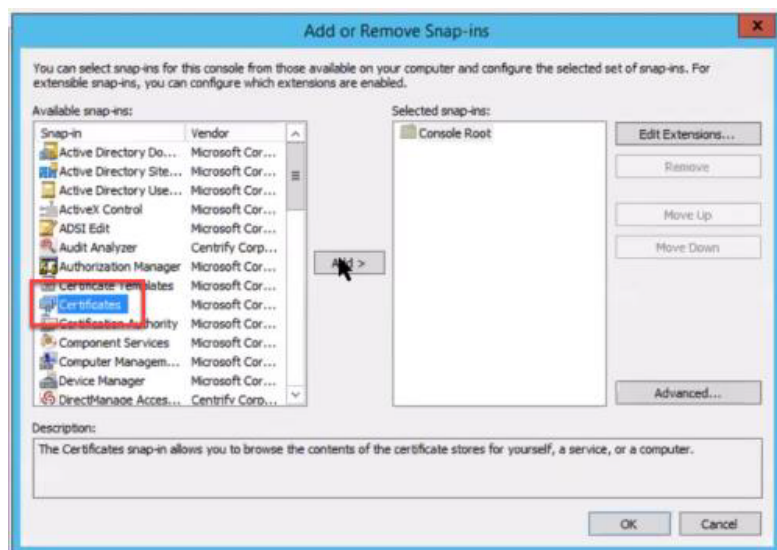
11. Scroll down to **Computer with Exportable Key**. Click **OK**.

The modified template is now ready for use through group policy.

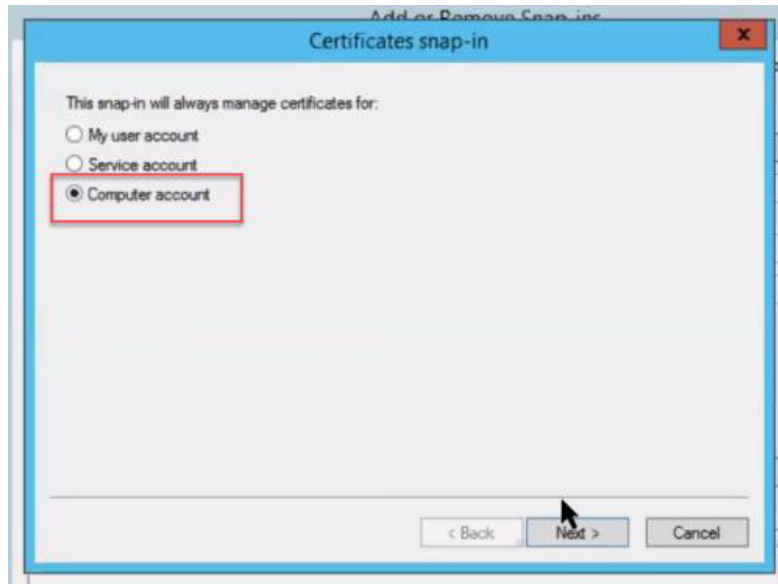
12. Close the **Certification Authority** console.

To generate a computer certificate for the Delinea Connector:

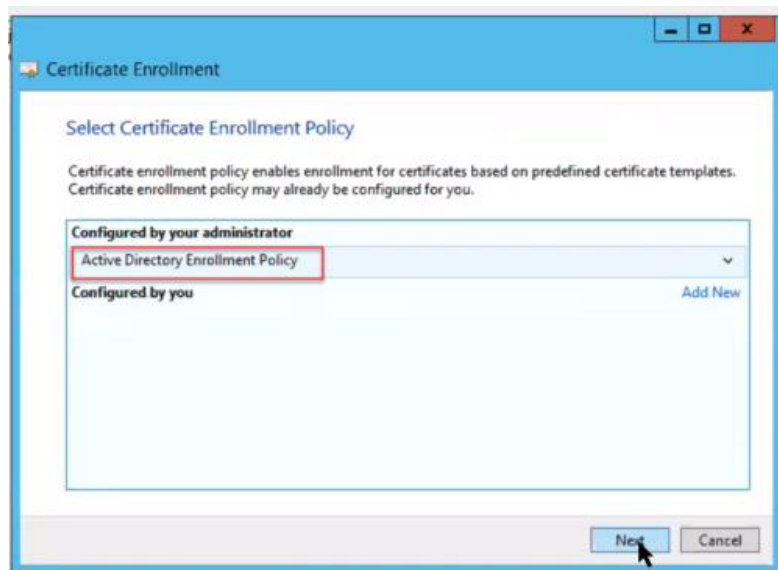
1. In the server where you are going to create the certificate, open the mmc . exe program.
2. In the MMC program, select **File > Add/Remove Snap-ins**. Add the **Certificates (Computer)** snap-in. Click **Add**.



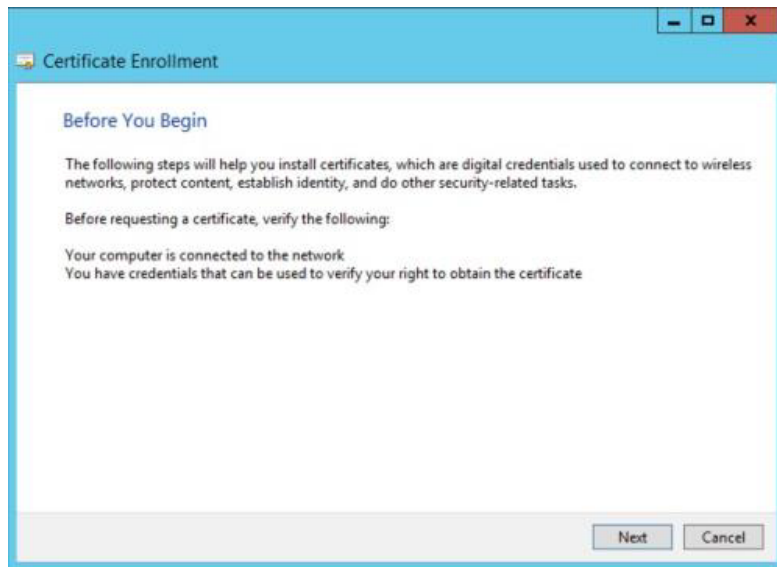
3. For the Certificates snap-in, choose **Computer account**. Click **Next**.



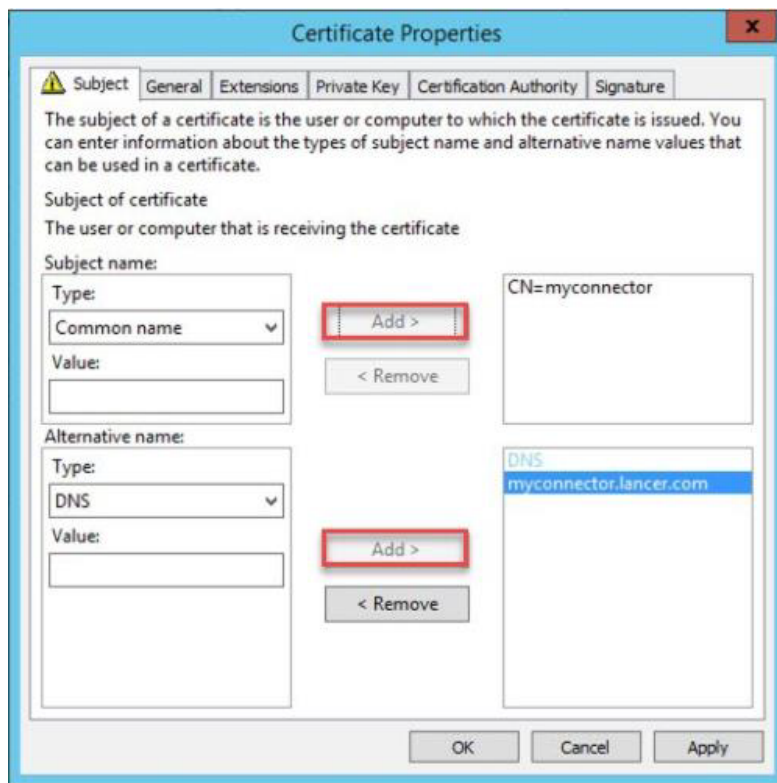
4. In **Select computer**, keep all the default values. Click **Finish**, then click **OK**.
5. Navigate back to the console. In **Console Root**, right-click **Personal**, then select **All Tasks > Request New Certificate**. Click **Next** on the **Certificate Enrollment** screen.
6. On the **Select Certificate Enrollment Policy** screen, ensure you have **Active Directory Enrollment Policy**. Click **Next**.



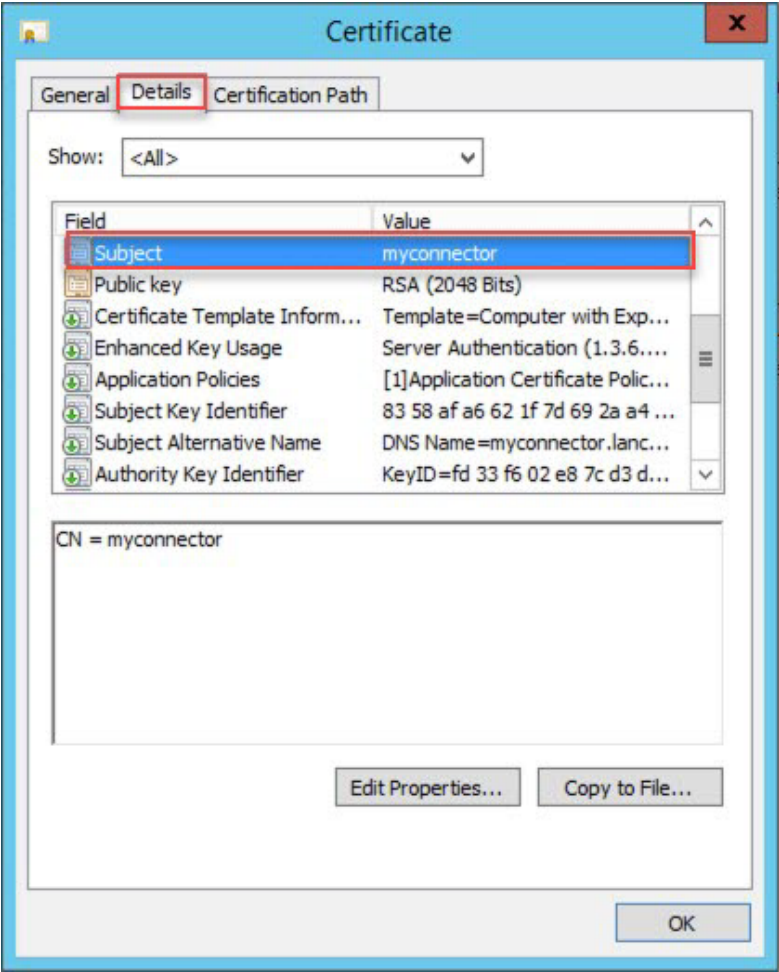
7. For **Request Certificate**, select **Computer with Exportable Key** and click the hyperlink directly below, **More information is required to enroll for this certificate**. Click [here](#) to configure settings.

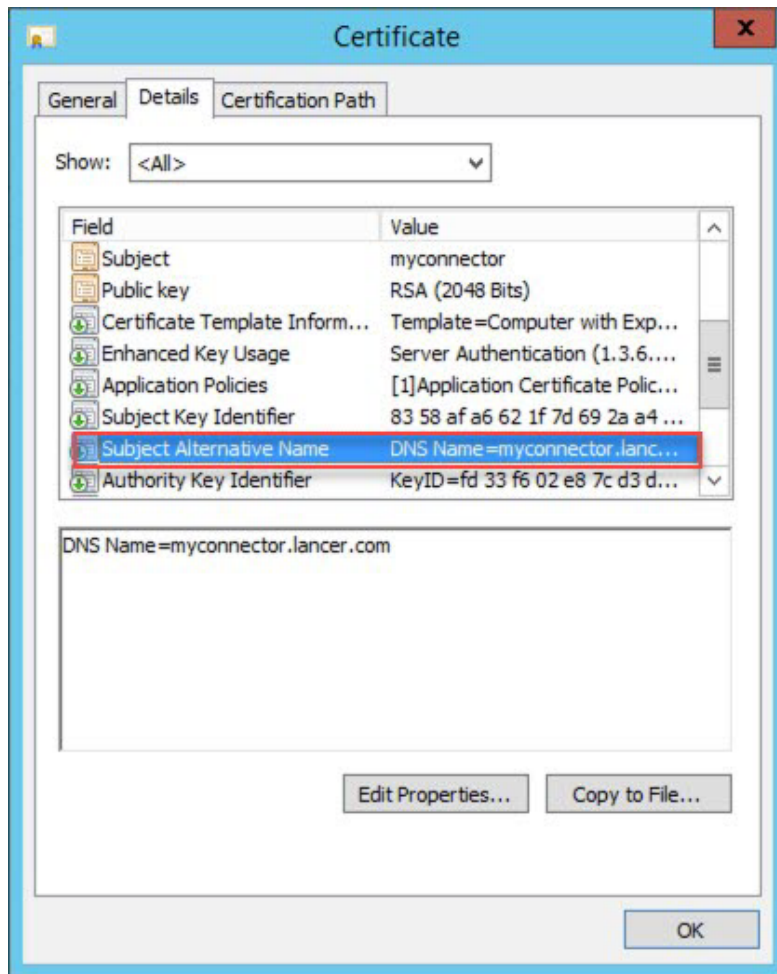


8. Press **Add** on both **Subject name** and **Alternative name** to move the set values to the right side. Click **OK**.



 **Note:** To obtain the **Subject name** and **Alternative name**, click the certificate details (subject name and subject alternative name).

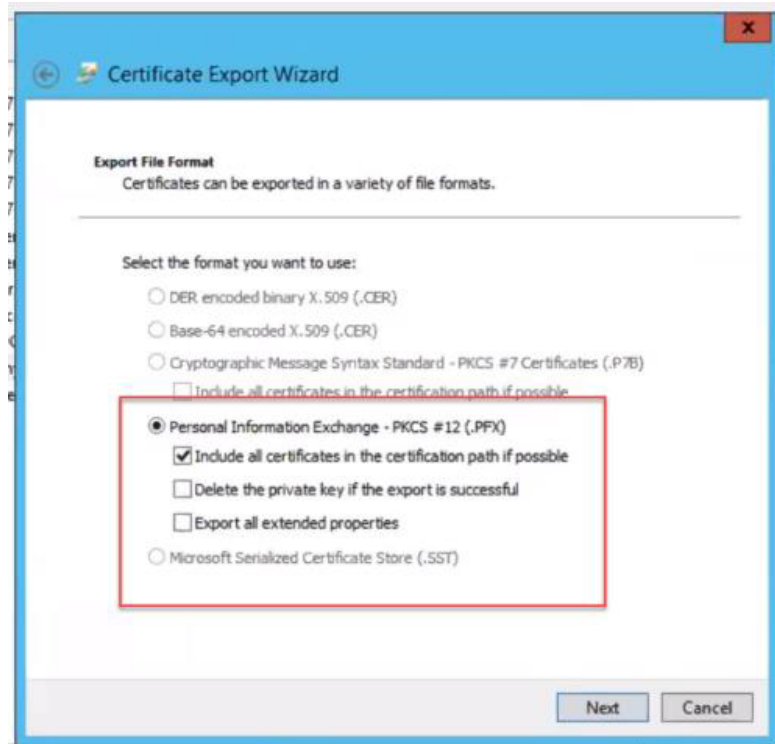




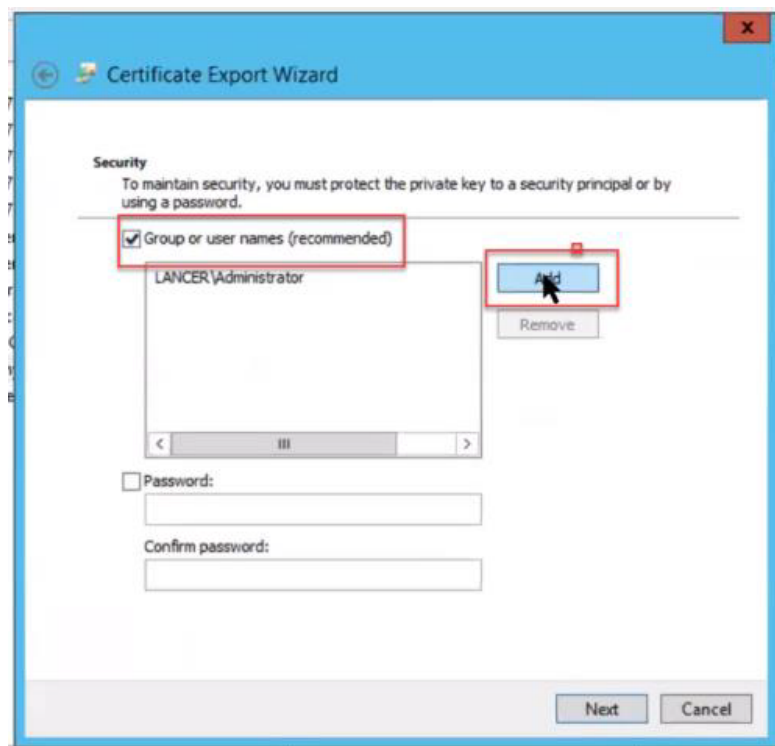
To export the certificate with the private key

Export the certificate and install it on the computer where you have installed the connector.

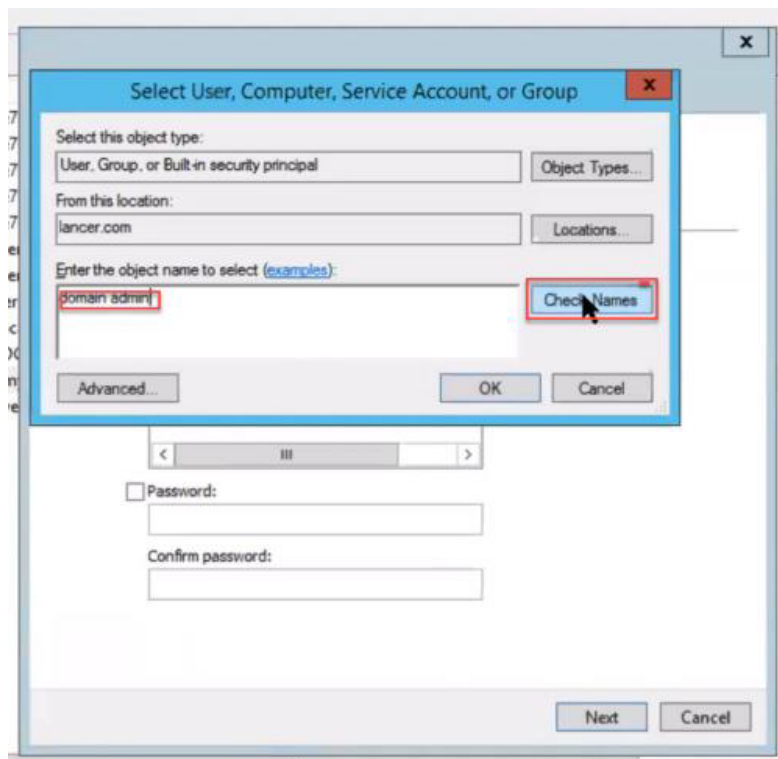
1. Under **Personal > Certificates**, right click the **Delinea** (or the name of the server) **Certificate** and select **Export**.
2. Click **Next**.
3. On the **Export Private Key** screen, select **Yes, export the private key** . Click **Next**.
4. For **Export File Format**, keep the default value, **Personal Information Exchange - PKCS # 12 (.PFX)**. Click **Next**.



5. On the **Security** screen, select **Group or user names (recommended)**. Click **Add**.



6. On the **Select User, Computer, Service Account, or Group** screen, in the field **Enter the object name to select (examples)**, enter **domain admin**. Click **Check Names**.



7. Click **OK**, then click **Next**.
8. For **File to Export**, give a name to the file and click **Save**.
9. Click **Next**.

Make a note of this location, because you will need it during setup (for example, `c:\delinea\delinea.pfx`).

10. In the **Completing the Certificate Export Wizard** screen, click **Finish**.
11. A message dialog appears to say the export was successful. Click **OK**.

Joining Linux/UNIX Hosts to a Domain/Zone

You have completed the preparation of the environment and added existing users and groups to Active Directory. The steps up to this point have not affected the day-to-day activities of any UNIX/Linux users or groups and have not changed the configuration of any UNIX/Linux computers. The final step in the migration requires you to join UNIX/Linux computers to the Active Directory domain. This step does have the potential to affect end-users.

This section describes how to complete the migration by joining the target set of computers to an Active Directory domain and a Privilege Control zone.

Using Adjoin on New Computers

You can run the `adjoin` command interactively or in a script to join UNIX/Linux computers to Active Directory. One advantage to using the `adjoin` command is that it enables you to add the join operation to the steps for building a

new UNIX/Linux computer. For example, if you have a process for provisioning a new UNIX/Linux computer, you can add an `adjoin` step that allows the new UNIX/Linux computer to join itself to Active Directory. Provisioning new computers to join the domain when they are built ensures that there are no new local users being defined on those UNIX/Linux computers.

Running Adjoin Requires UNIX and Active Directory Privileges

On UNIX, running `adjoin` requires you to log in as root, be a member of the wheel group, or have root equivalent privileges in the `sudoers` file. On Mac OS X computers, `adjoin` requires the administrator account and password.

Specifying the Required Options

The basic syntax for the `adjoin` command is:

```
adjoin [options] domain_name [--zone zone_name | --workstation]
```

The `domain_name` should be a fully-qualified domain name; for example, `sales.acme.com`. If you are using `adjoin` to provision new computers, there are several options you need to specify on the command line or in the script.

- Use the `--container` or `-c` option to specify the location for the computer account. Typically, you should use the organizational unit that you created for UNIX Servers and Workstation under the top-level UNIX organizational unit. It must be the location you used when you created the computer object. For example:
`-c "ou=UNIX Server and workstations,ou=UNIX"`
- Use the `--selfserve` or `-S` option to specify that you want the computer to join itself to the Active Directory domain.
- Use the `--zone` or `-z` option to specify the name of the zone to join. You must specify a zone name unless you are joining Auto Zone using the `--workstation` option.
- If you have a disjointed DNS environment where the Active Directory domain for the computer account does not match the name of the DNS domain, you must also specify the `--name` and `--alias` options. The `--name` option specifies the name of the Active Directory computer object and the `--alias` is the fully-qualified DNS name of the computer.
- Use the `--computerpassword` or `-x` option to specify the password of the previously created computer account. You must also specify either `--precreate` or `--selfserve`. If you don't specify the password, the default password is used.

For example, update your provisioning process for a new computer to include a command similar to the following:

```
adjoin -c "ou=UNIX Server and workstations,ou=UNIX" -S -z production arcade.net
```

For complete information about `adjoin` options, see the `adjoin` man page.

Pre-staging Before Using Adjoin on a New Machine

When joining a large AD environment, the join procedure can take up to dozens of minutes. This becomes a concern in some use cases, such as starting an Amazon EC2 instance that needs to join the domain to provide service.

To speed up the `adjoin` process, the `--prestage` option uses existing cache files instead of populating the cache from scratch.

Some preparation is required to take advantage of the `--prestage` option:

- Prepare a pre-staged cache directory on a joined machine.
- Copy the cache directory to the new machine.

Security Requirements

To use the `--prestage` option, ensure the following:

- Joined and new machine requirements:
 - The `--prestage` option can only be used between machines that have the same platform, architecture, and Authentication Service (Centrify DirectControl) release version installed.
 - The `adc1ient` cache data encryption feature cannot be enabled on the joined machine. See the `adc1ient.cache.encrypt` parameter.
- Pre-staged cache directory on joined machine requirements:
 - On a joined machine, create or designate a directory for the pre-staging cache files.
 - The directory must be in a safe path: all levels of parent directories must be owned by system accounts.
 - The directory cannot be either group or world writable.
- Content for the pre-staged cache directory on the joined machine:
 - Place the cache files (`dz.cache`, `dc.cache`, `gc.cache`, `.idx` and `kset`. files) in the specified directory.
 - Ensure the cache files are owned by system accounts.
 - Files cannot be either group or world writable.
 - Symlink is not allowed for the cache files.
- Zone hierarchy changes are not allowed between the staging directory and the new machine. This includes:
 - zone name change
 - zone GUID change
 - zone schema change

Preparing to Use the `--prestage` Option

Before using the `--prestage` option:

1. Create a directory on a joined machine. For example, `/pre`.
2. Stop `adc1ient` on that machine.
3. Copy the `/var/centrifydc/` directory to the pre-staged directory on the joined machine.

For example:

Copying the `/var/centrifydc/` directory to the pre-staged directory, `/pre`, places a copy of the required files in `/pre/centrifydc/`.

4. Verify the pre-staged directory on the joined machine contains all the `.idx`, `.cache`, and `kset`. files.
5. Copy the pre-staged directory to the new machine.

Use a method of your choice, such as `scp` or `sftp`.

This is done so the pre-staged files are available locally on the new machine.

6. Add the `--prestage` option to the `adjoin` command when adding the new machine. The syntax is:

```
-E | --prestage <directory>
```

For `<directory>`, substitute the path to the pre-staged directory on the new machine.

For example, if the pre-staged files are in the directory `/pre/centrifydc/`, use the following `adjoin` command:

```
adjoin -z <zone> -E /pre/centrifydc<domain>
```

Log On to Verify Authentication After Joining the Domain

As the final step in the initial migration, you should verify that authentication for an Active Directory user is successful. You can do this by logging in to the UNIX console using either the UNIX user name or the Active Directory User Principal Name for a user assigned to the UNIX Login role. When prompted, type the Active Directory password for the account. If you are able to log in using the Active Directory password, authentication is being handled by Active Directory and the user account has been successfully migrated.

You should also verify that you can log in remotely using a secure shell (ssh) connection and that you can use other services such as ftp.

If users have trouble logging in after a UNIX/Linux computer has joined the domain, it is typically because they are not assigned the UNIX/Linux Login role or do not have a valid UNIX/Linux profile in the zone. You can use the `Show Effective UNIX/Linux User Rights` command to check which users have profiles and what roles have been assigned to users who have access to the selected computer.

Using GPO on Platform

You can use Microsoft Group Policy Objects (GPO) to configure settings on PCS servers that have the Server Suite agent installed on the endpoints. With group policies, you can centrally manage computer and user configuration settings through GPO.

1. From the Delinea Marketplace, download GPO templates. The file name is `Delinea-PCS-GP.zip`.

For information about the Marketplace, see ["Integrations and Marketplace" on page 587](#).

2. Install and implement the GPO templates according to the instructions in Server Suite documentation:

- [Server Suite Group Policy Overview](#)
- [Group Policy Guide](#)
- [Adding Administrative Templates to a Group Policy Object](#)

Using Commands

This page gives examples and details about the commands that can be specified as part of a Granular Privilege Elevation PCS policy. For an overview and step-by-step instructions on how to create this type of policy, see [Step 10: Set Up PCS Policies](#) in the *PCS End-to-End Installation and Run Guide*.

Controlling Access to Commands

In a standard UNIX shell environment, an ordinary user account can execute a large number of common command-line programs without any special privileges, and one or more administrative accounts, such as root, are required to

execute commands that perform privileged operations. If ordinary users need to execute any of the commands requiring administrative privileges, they might have to switch to an administrative account that requires them to know the password for a privileged user, or they might be granted access by configuration settings in a `sudoers` file.

For Linux and UNIX computers managed by Delinea Platform, however, you can define command access rights to tightly control the specific commands users can execute. You can also refine those rights to only allow specific arguments to be used or to require an executable to be located in a specific directory.

There are no predefined rights for commands. Therefore, only the specific command access rights you define will be available for you to add to roles.

What Command Rights Provide

Command access rights identify the specific commands that can be executed on a Linux or UNIX computer by a user assigned the role to which the rights are added. Command rights also specify whether the commands defined in the right are executed under the user's own account or using another user account.

There are two primary reasons for defining command rights:

- To **grant access** to specific commands that must be executed with elevated privileges.
- To **restrict access** to only allow specific commands to be executed.

Granting Access Using Command Rights

The most common reason for creating a command right is to allow users to execute commands that require privileges not granted to a standard UNIX user account. For example, you might want to grant some users permission to run command-line programs that require root privileges to better manage their own computers.

With this type of command right, most commands are executed in the default shell environment with ordinary user privileges. When users assigned to a role with this type of command right want to use their elevated privileges, they invoke the command they have been granted access to using the `dzdo` command. This type of command right is similar to configuring privileges in a `sudoers` file, then invoking a command using `sudo`.

This type of command right is appropriate for UNIX users who have a standard shell environment and only need elevated rights to perform specific tasks.

Examples of Windows Elevated Privilege Commands and Apps

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

Privilege Elevation Command Name	Application and Arguments	Path
Server Manager	ServerManager.exe	Standard system path
Service Control Manager	sc.exe	Standard system path
Microsoft Management Console (MMC)	mmc.exe	Standard system path

Examples of Linux Elevated Privilege Commands and Apps

Here are some examples of Linux elevated privilege commands and applications you could include in a command group named "Linux commands" or something similar.

In these command definitions, glob pattern matching is used to expand any wildcard expressions. For more information, see "About Glob Expressions" on page 644.

Privilege Elevation Command Name	Command	Argument	Match Path	Description
Edit SSH server config	vi	/etc/ssh/sshd_config	Standard user path	Allows the granted user to edit the SSH server's config file, but nothing else
Edit SSH	vi	/etc/ssh/*_config	Standard user path	Allows the granted user to edit any SSH-related configuration
Change firewall	iptables	-A INPUT -s *-j ACCEPT	Standard system path	Allows the granted user to change Linux firewall rules so specified hosts can make network connections
Restart PostgreSQL	systemctl	restart postgresql	Standard system path	Allows the granted user to restart the PostgreSQL service

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

Linux PCS Template Commands

Privilege Elevation Command Template	Command	Argument	Match Path	Run Command As	Description
Any command (Root Equivalent)	*		Specific path	Root user	Allows the user to run any command as root.
Delinea PCS - adcdiag	adcdiag	*	Specific path	Root user	Allows the user to execute adcdiag with any argument. The adcdiag diagnostic tool is used to check whether the environment is ready for MFA.

Privilege Elevation Command Template	Command	Argument	Match Path	Run Command As	Description
Delinea PCS - adflush	adflush	*	Standard system path	Root user	Allows the user to execute adflush with any argument. The adflush tool refreshes its local cache, pulling the latest from the PCS tenant.
Delinea PCS - adinfo	adinfo	*	Standard system path	Root user	Allows the user to execute adinfo with any argument. The adinfo diagnostic tool is used to provide feedback of the agent's AD status.
Delinea PCS - dzinfo	dzinfo	*	Specific path	Root user	Allows the user to execute dzinfo with any argument. The dzinfo diagnostic tool is used to provide feedback of the commands available to the user.
System - env	env	*	Standard user path	Root user	Allows the user to execute the env command without any arguments.
System - groups	groups	*	Standard user path	Root user	Allows the user to execute the groups command with any argument.
System - httpd	service	httpd* *	Standard user path	Root user	Allows the user to execute service httpdwith any argument.
System - id	id	*	Standard user path	Root user	Allows the user to execute id with any argument.
System - ls	ls	*	Standard user path	Root user	Allows the user to execute ls with any argument.
System - mkdir	mkdir	*	Standard user path	Root user	Allows the user to execute mkdir with any argument.
System - mv	mv	*	Standard user path	Root user	Allows the user to execute the mv command with any argument.

Privilege Elevation Command Template	Command	Argument	Match Path	Run Command As	Description
System - NO Bash	!bash		Standard user path	Root user	Prevents the user from executing bash.
System - NO su	!su		Standard user path	*	Prevents the user from executing su to switch to any other user account.
System - NO su to root	!su	- root	Standard user path	Root user	Prevents the user from executing su to switch to the root user account.
System - rm	rm	*	Standard user path	Root user	Allows the user to execute rm with any argument.
System - stat	stat	*	Standard user path	Root user	Allows the user to execute stat with any argument.
System - touch	touch	*	Standard user path	Root user	Allows the user to execute touch with any argument.

About Linux Match Paths

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

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

Each match path maps to one or more of the binary directories on Linux systems as follows:

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

Linux uses each directory for a specific, as follows (text from Linux help output):

- `/bin`: For binaries usable before the `/usr` partition is mounted. This `/bin` directory is used for trivial binaries used in the very early boot stage or ones that you need to have available in booting single-user mode. Think of binaries like `cat`, `ls`, and so forth.
- `/sbin`: Same, but for binaries with superuser (root) privileges required.
- `/usr/bin`: Same as first, but for general system-wide binaries.
- `/usr/sbin`: Same as above, but for binaries with superuser (root) privileges required.

About Glob Expressions

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

The glob standard gives special meaning to a few characters:

Glob Character	Description	Example Pattern	Example Results
* (asterisk)	Matches any number of characters, including zero	<code>app*</code>	application apple app
		<code>b*d</code>	bad bud bid bGd bland before we sighted land
? (question mark)	Matches any one character	<code>b?d</code>	bad bud bid bGd
[] (brackets)	Can contain any number of characters and matches exactly one character if it's contained between the brackets.	<code>the*brown*f?x j [au]*</code>	the quick brown fox jumps the sly, silly brown fox jabbered

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

Managing Agents

This page gives information you might need to know in the course of managing the agents installed as part of your Delinea Platform deployment.

Installing Agents on Computers to be Managed

This section describes the recommended steps for deploying Privilege Control software on the non-Windows computers that you want to add to Active Directory. The section also describes the alternatives you can use to install agent packages on non-Windows computers, including using native Linux installers to install Privilege Control packages manually and automatically.

System Requirements

Be sure the computers where you are installing the Delinea Agent are running one of the supported operating systems. See "Supported Operating Systems for Agents" on page 610.

About the Deployment Process

There is no technical requirement that you only work with a subset of computers at a time, but the process of checking computers for potential problems and resolving open issues is more manageable when applied to a subset of computers. It is also more practical to migrate user populations in stages rather than all at once. After you step through the process a few times, you'll be able to anticipate and resolve potential issues more quickly and move into a more rapid deployment model.

Selecting a Target Set of Computers

As a first step in preparing to install Privilege Control software, select a target set of computers on which to deploy. The target set can be based on any criteria you choose. In many organizations, new software must always be installed in the development environment first, then in the pre-production environment, before it can be deployed in the production environment. If your organization has this type of requirement, the first target set of computers would be the computers in the development environment.

Other possible candidates for the target set might be computers that:

- Have been identified for changes by an audit finding
- Are in the same physical location, such as a particular data center
- Share common attributes, such as all Red Hat Linux computers or all of the servers in a Web farm
- Are used by a particular department, project, or line of business
- Have a common set of users who need access to the computer resources

After you have identified a target set of computers, you are ready to begin the deployment. You should notify the user community that you are planning to install software on the target set of computers. For example, you may want to notify users by sending out an email message similar to the sample provided in *Preliminary software delivery notification email template*.

You can use adcheck to check whether those computers have any issues that need to be resolved before you install new software on them. Checking the environment before you install helps to reduce change control issues.

Options for Deploying Privilege Control Agent Packages

To deploy Privilege Control agent packages, you can choose from the following options:

- Run the agent installation script locally on any computer and respond to the prompts displayed.
- Create a configuration file and run the installation script remotely on any computer in silent mode.
- Use the install or update operations in the native package installer for your operating environment.
- Use a commercial or custom software distribution tool.

If you want to use one of these installation options and need more information, see the appropriate section.

Installing Interactively on a Computer

The Privilege Control Agent installation script `install.sh` automatically checks the operating system, disk space, DNS resolution, network connectivity, and other requirements on a target computer before installing. You can run this script interactively on any supported UNIX or Linux computer and respond to the prompts displayed.

To install Privilege Control software packages on a computer interactively:

1. Log in or switch to the root user if you are installing on a Linux or UNIX machine.
2. Change to the appropriate directory that contains the Privilege Control Agent package you want to install.

For example, to install an agent on a Linux computer from a downloaded Privilege Control ISO or ZIP file, change to the `Agent_Linux` directory:

```
cd Agent_Linux
```

Similarly, if you are installing on a Solaris, HP-UX, AIX or other UNIX computer, change to the `Agent_Unix` directory.

If you downloaded individual agent packages from the Delinea Download Center, unzip and extract the contents. For example:

```
gunzip -d os-arch.tgz
tar -xf os-arch.tar
```

3. Run the `install.sh` script to start the installation of the agent on the local computer's operating environment. For example:

```
./install.sh
```

4. Follow the prompts displayed to select the services you want to install and the tasks you want to perform. For example, you can choose whether you want to:

- Perform a default installation.
- Perform a custom installation by selecting the specific packages to install.
- Join a domain automatically at the conclusion of the installation.

Depending on your selections, you may need to provide additional information, such as the user name and password for joining the domain.

Installing Silently Using a Configuration File

Installing without user interaction enables you to automate software delivery and the management of remote computers. If you want to install files without any user interaction, you can run the `install.sh` script silently invoking the script with the appropriate command-line arguments. You can also customize the packages installed and other options by creating a custom configuration file for the installer to use.

- To see the `install.sh` silent mode and other command line options, enter:

```
install.sh -h
```

- To install Authentication & Privilege default packages and configuration options silently, run:

```
install.sh --std-suite
```

- To install Authentication & Privilege and Audit & Monitoring default packages and configuration options, run:

```
install.sh --ent-suite
```

- To install a customized set of packages that all have the same version number, run:

```
install.sh -n
```

About the Sample Configuration Files

You can customize the `install.sh` execution script. There are two sample configuration files for installing software packages silently. These sample configuration files are located in the same directory as the `install.sh` script:

- `centrify-suite.cfg`
- `centrifydc-install.cfg`

If you want to customize the packages installed or other configuration options, you can modify the sample `centrify-suite.cfg` or `centrifydc-install.cfg` file.

The `centrify-suite.cfg` file is used when you run `install.sh` with the `--std-suite` or `--ent-suite` options. If you run `install.sh --std-suite` or `install.sh --ent-suite` with a customized version of the `centrify-suite.cfg` file, you can selectively install compatible add-on packages that do not have the same version number as the core Privilege Control Agent.

Alternatively, you can run `install.sh -n` with a customized version of the `centrifydc-install.cfg` file to install the agent and add-on packages if they all have the same version number.

If you run the `install.sh` script silently and it cannot locate the `centrify-suite.cfg` or `centrifydc-install.cfg` file to use, default values defined directly in the script itself are used.

Setting the Parameters in a Custom Configuration File for the Installation Script

If you want to specify values for the `install.sh` script to use, edit the sample `centrify-suite.cfg` or `centrifydc-install.cfg` file in its default location before invoking the `install.sh` script in silent mode.

The parameters in the `centrifydc-install.cfg` or `centrify-suite.cfg` file are the same, except that the `centrify-suite.cfg` file is used when installing a set of services to allow packages with different version numbers to be installed together. Because you should not modify the compatibility defined in the `centrify-suite.cfg` file, those parameters are not included in the table.

To customize the installation using the `centrifydc-install.cfg` or `centrify-suite.cfg` file:

Privilege Control for Servers

Specify the operation to perform. The valid settings are:

- Y to install the Privilege Control Agent for *NIX and any other Privilege Control software packages if they are not already installed on the local computer.
- U to update older versions of the Privilege Control Agent for *NIX and any other Privilege Control packages you have installed. The update option only updates software from one major release version to another. It does not update the software if the major release version is same between packages.
- R to reinstall or repair the Privilege Control Agent for *NIX and any other Privilege Control packages you have installed. You can reinstall packages that have the same major release version but different build number or repair packages by installing an older version of the package.
- E to remove the software currently installed.
- K to keep current software unchanged.

Set this parameter to Y to install or to U to update the Privilege Control Agent for *NIX and other packages.

If you want to install or update other packages, select the operation to perform for each package. For example, to update the Privilege Control Kerberos package and keep the current Privilege Control LDAP proxy service, you might specify the following:

```
CentrifyDC_krb5="u"  
CentrifyDC_ldaproxy="k"
```

These additional packages might have dependencies or require a specific version of the Privilege Control Agent for *NIX to be installed.

Before installing or updating additional packages silently, review the information in the Server Suite [Upgrade and Compatibility Guide](#).

Parameter	Description
ADCHECK	Indicate whether you want to run the adcheck program to check the configuration of a local computer and its connectivity to Active Directory. The <code>install.sh</code> script calls <code>adcheck</code> twice. After the first call, <code>adcheck</code> performs several required pre-installation steps to make sure you can install the Centrify Agent on the host computer. These steps are mandatory and cannot be skipped. However, the second call to <code>adcheck</code> is used to perform post-installation steps to make sure the agent has been installed successfully. The second set of checks is optional and can be skipped. Set this parameter to Y if you want to run <code>adcheck</code> after installing. For non-interactive installations, the default is N.
ADLICENSE	Indicate whether you want to install licensed features. Set this parameter to Y if you have purchased and installed license keys. If you downloaded and want to install unlicensed Centrify Express agents, set this parameter to N.

Parameter	Description
GLOBAL_ZONE_ONLY	Specify whether you want to install the agent in a Solaris 10 global zone and no other zones. Set this parameter to Y only if you are running the <code>install.sh</code> script on a Solaris 10 computer and want to install the agent in the Solaris 10 global zone and none of your non-global zones. In most cases, you only set this parameter to Y if you use sparse root zones. The default setting for this parameter is N so that the agent is installed in all Solaris zones. If the script is not running on a Solaris 10 computer, this parameter is ignored.
ADJOIN	Indicate whether you want to attempt to join an Active Directory domain in non-interactive mode. Set this parameter to Y to attempt to join the domain automatically. Set this parameter to N to manually join the domain after installation.
ADJ_FORCE	Overwrite the information stored in Active Directory for an existing computer account. Set this parameter to Y to replace the information for a computer previously joined to the domain. If there is already a computer account with the same name stored in Active Directory, you must use this option if you want to replace the stored information. You should only use this option when you know it is safe to force information from the local computer to overwrite existing information.
ADJ_TRUST	Set the Trust for delegation option in Active Directory for the computer account. Trusting an account for delegation allows the account to perform operations on behalf of other accounts on the network.
DOMAIN	Specify the domain to join, if you set the ADJOIN parameter to Y. Set this parameter to the name of a valid Active Directory domain.
USERID	Specify the Active Directory user name to use when connecting to Active Directory to join the domain. Set this parameter to a valid Active Directory user name.
PASSWD	Specify the password for the Active Directory user name you are using to connect to Active Directory. Set this parameter to the password for the Active Directory user name specified for the USERID parameter.

Parameter	Description
COMPUTER	Specify the computer name to use for the local host in Active Directory. Set this parameter to the computer name you want to use in Active Directory if you don't want to use the default host name for the computer.
CONTAINER	Specify the distinguished name (DN) of the container or Organizational Unit in which you want to place this computer account. The DN you specify does not need to include the domain suffix. The domain suffix is appended programmatically to provide the complete distinguished name for the object. If you do not specify a container, the computer account is created in the domain's default Computers container. Note that the container you specify must already exist in Active Directory, and you must have permission to add entries to the specified container.
ZONE	Specify the zone to which you want to add this computer.
SERVER	Specify the name of the domain controller to which you prefer to connect. You can use this option to override the automatic selection of a domain controller based on the Active Directory site information.
DA_ENABLE	Indicate whether you want to automatically enable the auditing service on the local computer. The valid settings are: Y if you want to enable auditing with the default auditing configuration. N if you don't want to enable auditing. K if you are upgrading and want to keep your current auditing configuration unchanged.
DA_X_ENABLE	Indicate whether you want to automatically enable the Linux desktop auditing service on the local computer. The valid settings are: Y if you want to desktop enable auditing with the default auditing configuration. N if you don't want to enable desktop auditing. K if you are upgrading and want to keep your current auditing configuration unchanged
DA_INST_NAME	Specify the name of an auditing installation if you set the DA_ENABLE parameter to Y.

Parameter	Description
REBOOT	Indicate whether you want to automatically restart the local computer after a successful installation. Set this parameter to Y if you want to automatically restart the local computer or to N if you don't want the computer restarted automatically.
INSTALL	
UNINSTALL	Specify whether you want to forcibly uninstall all installed packages.

For example, you can edit the `centrifydc-install.cfg` or `centrify-suite.cfg` file to silently install the Privilege Control Agent for *NIX, join the domain, and automatically reboot the computer at the completion of the installation process with a file similar to this:

```

ADCHECK="N"
ADLICENSE="Y"
# solaris 10 -G option, installation in global zone only
GLOBAL_ZONE_ONLY="N"
ADJOIN="Y"
ADJ_FORCE="N"
ADJ_TRUST="N"
DOMAIN="sample.company.com"
USERID=administrator
PASSWD="securepassword123"
# COMPUTER=my_host_name
# CONTAINER="my_computers"
ZONE="global_zone"
# SERVER=server_name
DA_ENABLE="N"
DA_INST_NAME=""
REBOOT="Y"
# Install the core agent package
INSTALL="Y"

# Skip installation for other packages
CentrifyDC_nis=
CentrifyDC_krb5=
CentrifyDC_ldapproxy=
CentrifyDC_openssh=

```

```
CentrifyDC_web=  
CentrifyDC_apache=  
CentrifyDC_idmap=  
CentrifyDA=
```

This sample configuration file does not install any of the Privilege Control add-on packages. You can also use the configuration file to silently install or update selected packages. For example, to update the LDAP proxy service and OpenSSH on a computer, you would modify the configuration file to indicate that you want to update those packages:

```
CentrifyDC_ldaproxy="U"  
CentrifyDC_openssh="U"
```

Customizing the Return Codes for the Installation Script

Normally, when you run the `install.sh` script silently, the script returns an exit code of 0 if the operation is successful. If you want the script to return exit codes that indicate whether the operation performed was a successful new installation, a successful upgrade, a successful uninstall, or there were errors preventing installation, you can also use the `custom_rc` option. For example:

```
install.sh -n --custom_rc
```

When you specify this option, the following return codes that are defined in the `install.sh` script are used to provide more detailed information about the result:

Return Code	Description
CODE_SIN=0	Successful installation
CODE_SUP=0	Successful upgrade
CODE_SUN=0	Successful uninstallation
CODE_NIN=24	Did nothing during installation
CODE_NUN=25	Did nothing during uninstallation
CODE_EIN=26	Error during installation
CODE_EUP=2	Error during upgrade
CODE_EUN=2	Error during uninstallation
CODE_ESU=29	Error encountered during setup; for example, the UID is not the root user UID, the operating environment is not supported or not recognized, or the script is executed with invalid arguments

Using Other Automated Software Distribution Utilities

You can also install Privilege Control software using virtually any automated software distribution framework. For example, you can use software delivery offerings from Chef, Puppet, Ansible, SaltStack, and so on to deliver Privilege Control software to remote computers. You can also use any custom software delivery tools you have developed specifically for your organization. If you use a commercial or custom software distribution mechanism, review the release notes text file included with the Agent package for platform-specific installation details.

About the Files and Directories Installed on the Agent

When you complete the installation, the local computer is updated with the following directories and files for the core Privilege Control Agent for *NIX:

Directory	Contents
/etc/centrifydc	The agent configuration file and the Kerberos configuration file.
/usr/share/centrifydc	Kerberos-related files and service library files used by the Centrify Agent to enable group policy and authentication and authorization services.
/usr/sbin /usr/bin	Command line programs to perform Active Directory tasks, such as join the domain and change a user password.
/var/centrify	Directories for temporary and common files that can be used by the agent.
/var/centrifydc	Before joining the domain, the directory contains basic information about the environment, such as the IP address of the DNS server and whether you installed licensed or express agent features. After you join the domain, several files are added to this directory to record information about the Active Directory domain the computer is joined to, the Active Directory site the computer is part of, and other details.

Depending on the components you select during installation, additional files and directories might be installed or updated. For example, if you install Enterprise Edition, the computer is updated with additional files and directories for auditing.

Joining an Active Directory Domain at a Later Time

At this point, you have delivered the software to target computers, but not changed their configuration. Users still have exactly the same access as they did before installing Privilege Control software. The computer's configuration changes only happen when the computer joins an Active Directory domain. Joining the domain is what activates Privilege Control software.

You have the option to automatically join an Active Directory domain when you install Privilege Control Agents with the `install.sh` script. In most cases, however, you should not do so unless you have already planned your user migration and created your initial zones. Typically, it is best to analyze the user population and prepare for migration before joining the domain to ensure minimal disruption of user activity and ease the transition to new software. Over time, as you become more familiar with the migration process and refine your zone design, you can adapt the steps to suit your organization.

If you want to join the domain at the same time you deploy the Privilege Control software, you should do the following before you install files on the UNIX computers:

1. Download the Privilege Control software for all platforms or the subset of platforms you intend to support.
2. Analyze existing user and group accounts.
3. Identify your zone requirements and create the initial zone design.
4. Migrate users and groups into the appropriate zones and role assignments.
5. Use the `install.sh` script or a custom script to install Privilege Control Agents and join the domain.

The additional steps are described in the next sections. You can also manually join a domain at any time after installation by using the `adjoin` command.

Upgrading the Linux Agent

To upgrade the Linux agent:

1. Log in to your Linux server as root user.
2. Create a folder (for example, `delinea-agent`) and extract the download package to the folder:

```
# mkdir delinea-agent
# tar -xzf rhel6-x86_64.tgz -C delinea-agent/
```

3. Navigate to the folder that you created in the previous step:

```
# cd delinea-agent/
```

4. Upgrade the Linux Agent:

```
# ./agent_setup.sh --upgrade
```



Note: The script has several options you can specify if needed. For more information, see the online documentation by running this command: `# ./agent_setup.sh --help`

Uninstalling a Linux Agent

To uninstall a Linux agent:

1. Log in to your Linux server as root.
2. Create a folder (for example, `delinea-agent`) and extract the download package to the folder.

```
# mkdir delinea-agent
# tar -xzf rhel6-x86_64.tgz -C delinea-agent/
```

3. Navigate to the folder you created in the previous step:

```
# cd delinea-agent/
```

4. If the machine is currently joined to a domain, leave the domain.

```
# adleave
```

If you are joined to a domain, and you do not leave it before proceeding with the uninstall command, a forced local leave will be performed when uninstalling, while the computer account will remain in AD.

5. Uninstall the Linux Agent:

```
# ./agent_setup.sh --uninstall
```

AD Orphan Object Cleanup Script

This topic describes the AD Orphan Object Cleanup script. This script runs on Windows computers and can be used to automate removal of obsolete items in Active Directory (AD). The script finds and deletes all user, group, and computer profiles that no longer have a corresponding Active Directory account on all managed computers in each zone.

Installing the PowerShell Access Module

This section explains how to download and install the Windows PowerShell Access Module, which you will need to run the AD Orphan Object Cleanup script. The script is included as part of the PowerShell Access Module.

You can download the access module for PowerShell as a separate package from the Delinea Download Center under Software Development Kits.

After you have downloaded the compressed file to your computer, extract the files and run the setup program to install the access module for PowerShell files.

To use the authentication and privilege elevation module for Windows PowerShell on a Windows Server server-core computer, you must first install Windows PowerShell, version 2.0 or later. Also, install the authentication and privilege elevation module for Windows PowerShell on a Windows Server Core environment in silent mode, due to a user interface limitation. Check the process exit code to see whether the installation succeeded or failed.

Server core is a minimal installation option that is available when you are deploying Windows Server. Server core includes most but not all server roles.

To run the setup program:

1. Download the access module for PowerShell as a separate package from the Delinea Download Center under Software Development Kits..
2. In the Windows File Explorer, right-click the downloaded file and select **Extract All**.
3. In the folder that contains the extracted files, double-click the setup program. For example, for the 64-bit version of the file, double click the `Centri fyDC_PowerShell-5.2.0-win64.exe` file.

Alternatively, you can install from the Microsoft Installer (.msi) file. For example, you might run the following command: `msiexec.exe /i "Centri fyDC_PowerShell-5.2.0-win64.msi" /norestart`.

The Welcome page appears.

4. Click **Next**. The License Agreement page appears.
5. Select **I accept the terms in the License Agreement**.
6. Click **Next**. The Location page appears.

7. Accept the default location.
8. Click **Next**.
9. Click **Install**.
10. Click **Finish**.

Creating and Using a Connection

Because the Delineaaccess module for PowerShell cmdlets manipulate objects in Active Directory, you must establish a connection with Active Directory before using the AD Orphan Object Cleanup script. To do that, you must specify a target domain or domain controller and the credentials to use when connecting to that domain or domain controller.

Once the credentials are set, all subsequent calls share that information—you do not have to provide the credential or the domain controller for any subsequent calls.

The following example illustrates how to use the administrator account to connect to the finance.acme domain, then add the user joe.doe to the Engineering zone:

```
PS C:\> Set-CdmCredential "finance.acme" "administrator"
PS C:\> Get-CdmCredential
Target      Type      User
-----
finance.acme Forest administrator@finance.acme
PS C:\> $zone = Get-CdmZone -Name "Engineering"
PS C:\> New-CdmUserProfile -Zone $zone -User "joe.doe@finance.acme" -Login "jdoe"
```

In this example, the cmdlets that get the zone and create the user profile use the credential that is cached by the Set-CdmCredential command. The Get-CdmCredential cmdlet shows what credentials are currently cached.

Confirming Licenses

The AD Orphan Object Cleanup script checks for a valid license before it runs. The license check succeeds only if there is at least one evaluation, workstation, or server license that has not expired.

If the license check fails, the script displays an error and stops running. Otherwise, the result is cached. The next time the script tries to access the same forest, it uses the cached result rather than performing the license check again.

The cache is only effective in one PowerShell console. If another PowerShell console runs the script accessing the same forest, the cmdlet in that console must perform a separate license check.

Running the Script

To run the AD Orphan Object Cleanup script:

1. Open the Delinea access module for PowerShell.
2. Verify you have permission to execute scripts by running Get-ExecutionPolicy. In most cases, the permission to execute scripts is restricted.

3. If necessary, use `Set-ExecutionPolicy` to allow execution. For example:

```
Set-ExecutionPolicy Unrestricted
```



Note: For more about execution policies and the options available, run the `get-help` command.

4. Verify you are in the directory where the script is located.
5. Run the script:

```
.\RemoveAllOrphans
```

Using the Default Windows PowerShell Console

Alternatively, you can use the default Windows PowerShell console. If you choose to use that console, run `import-module` with the path to the access module for PowerShell libraries before performing the above procedure. For example, if you installed the module in the default location, run the following command to import the Delinea access module for PowerShell:

```
import-module "C:\Program Files\Centrify\PowerShell\Centrify.DirectControl.PowerShell.dll"
```

Enabling Logging

For performance, logging for cmdlets is disabled by default, which means logging for the AD Orphan Object Cleanup Script is disabled. To enable logging, you must modify the registry on the computer where you are running the access module for Windows PowerShell.

To enable logging:

1. Run `regedit` to open the Registry Editor
2. Select the registry key `HKEY_CURRENT_USER > Software > Delinea`.
3. Right-click, then select **New > Key** and type `CIMS`.
4. Select the new `CIMS` key, right-click, then select **New > String Value** and give it the name `LogPath`.
5. Specify the path to the log file. For example, set the value to `C:\Temp\Log`.
6. Select the new `CIMS` key, right-click, then select **New > DWORD (32-bit) Value** and give it the name `TraceLevel`.
7. Specify the level of detail to write to the log file. The valid settings are:
 - 0 - disable logging
 - 1 - log only error messages
 - 2 - log errors and warning messages
 - 3 - log errors, warnings, and informational messages
 - 4 - log all debugging and tracing messages

Troubleshooting PCS

This page provides help for issues and questions you might encounter while using Delinea Platform and PCS.

Can't Find Log Files

Before you can begin troubleshooting, you need to know where to find the Delinea Platform log files.

Delinea Connector

C:\Program Files\Delinea\Delinea Connector\log.txt

Delinea Platform Engine

C:\ProgramData\Delinea Engine\<engine_version>\log

Command Relay

Command Relay stores logs in two places.

- Abridged Log:
C:\ProgramDataC:\Program Files\Delinea Engine\<engine_version>\delinea\command-relay\<version>\log
- Detailed Log:
C:\ProgramData\Delinea\CommandRelay\Logs

Privilege Control Agent

- **Linux:**
/var/log/centrifydc.log
- **Windows (default location):**
C:\Program Files\Common Files\Centrify Shared\Logs\

You can change where the Windows agent log files are stored using Privilege Elevation Service Settings:

1. Open Delinea Agent Configuration.
2. In Privilege Elevation Service, click **Settings**.
3. Select the Troubleshooting tab and click **Options**.
4. In Log folder path, set the path as desired.
5. (Optional) You can also change the trace level in this Options dialog.

Connection and MFA Issues

This section gives solutions for issues related to multi-factor authentication (MFA) and connecting to the Delinea Platform.

Can't Connect to Delinea Platform

Unable to log in to the Delinea Platform instance.

Connection issues can be caused by improperly configured Integrated Windows Authentication (IWA).

Use the following command to verify whether IWA is working on your Delinea Platform host:

https://<connector_host_name>:<https_port>/iwa/sitecheck

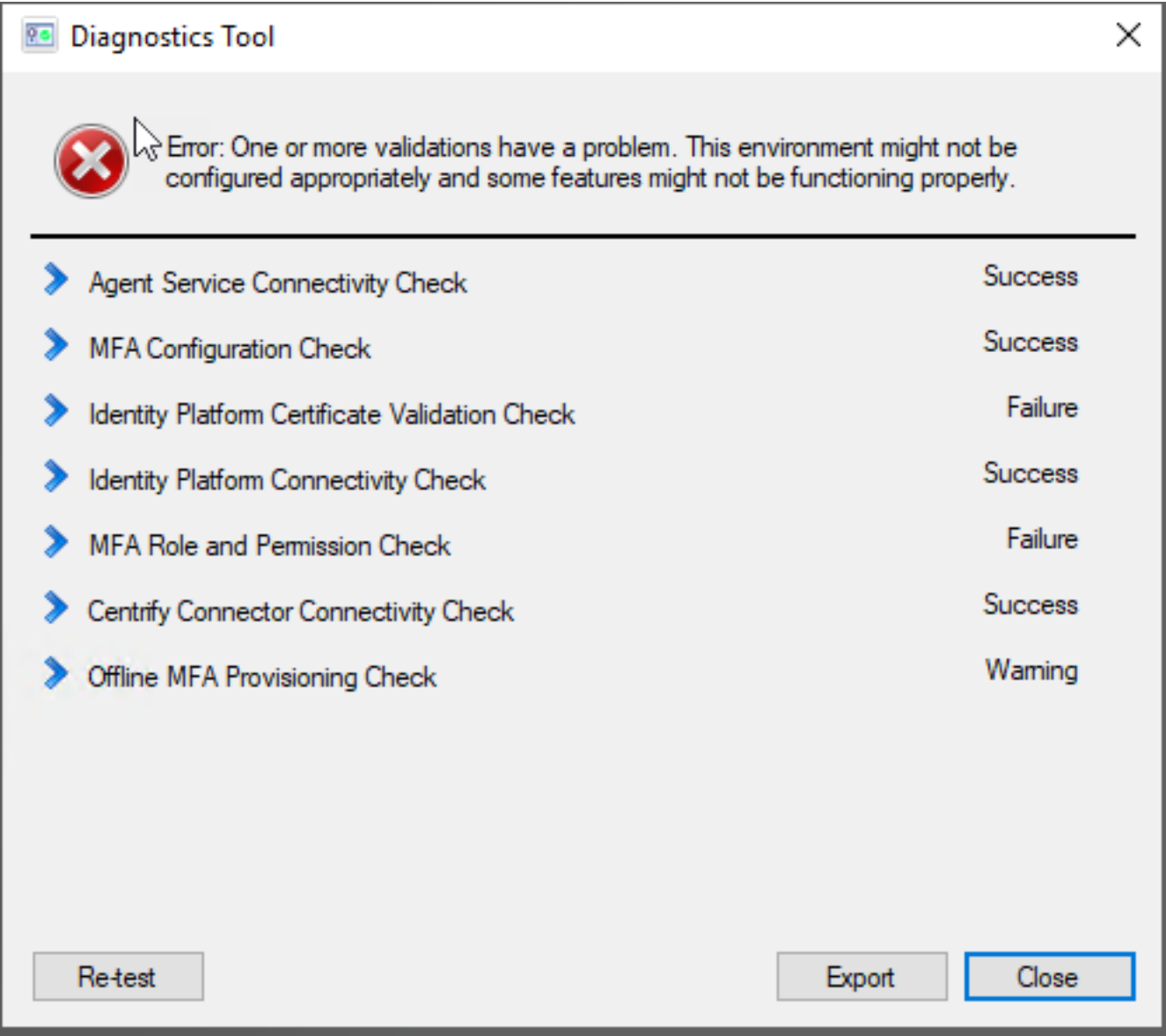
For details, see [Verifying IWA Over HTTPS](#).

 **Note:** The command `/iwa/ping` can also be used, but `/iwa/sitecheck` gives more information.

Windows Diagnostics Error for MFA

The Windows Diagnostics Tool produces an error message like the following:

"Error: One or more validations have a problem. The environment might not be configured appropriately and some features might not be functioning properly."



The error message is incorrect. It indicates erroneously that MFA is not working for PCS, when MFA is actually working. You can ignore this message.

MFA Zero Pass-Through Not Working

When configuring multi-factor authentication, you can set the pass-through duration to zero in an authentication profile. This pass-through setting should prevent any time from elapsing before a user is prompted again for MFA authentication. However, when privilege elevation is done with an MFA authentication profile set, the "no pass-through" setting is not honored.

The command `dzdo` is used to perform commands with privilege elevation. The issue occurs because, by default, `dzdo` has an authentication timeout interval of 5 minutes. This means that once `dzdo` has been authenticated, it does not have to authenticate again for 5 minutes. This 5-minute interval overrides the intended effect of setting the pass-through interval to zero.

To solve the issue, you must force `dzdo` to use an authentication timeout of 0, to match the pass-through interval. In the configuration file `/etc/centrifydc/centrifydc.conf` on the Linux agents, uncomment the parameter `dzdo.timestamp_timeout` and set it to 0.

DirectControl Authentication Not Working on *nix

On UNIX/Linux systems, when the directory `/var` is NFS mounted, DirectControl may not work properly.

Resolution:

Do not mount `/var` on NFS.

Policies

This section gives solutions for issues related to PCS authentication policies. For information about these policies, see [Step 10: Set Up PCS Policies](#).

Can't Find User for Subjects

Issue:

When searching for a known user to add as a subject for a PCS policy, the user's name does not appear, or no user names appear.

Resolution:

1. Open the Delinea Connector Configuration UI.
2. On the Status tab, look at the **Last connection result**.
 - If the message is "Connector is not available," select the Connector tab and click **Start**.
 - If the message is "Successful" but the **Last connection time** was a long time ago, select the Connector tab and click **Stop**.
When the connector stops, click **Start**. It might take several seconds for the connector to stop and start.
3. If your known user or all users are still not showing up in your search to a policy target, check the Connector logs. Contact Delinea support if necessary.

Policy Endlessly Activating or Deactivating

Issue:

A policy is stuck in Activating or Deactivating status.

Cause:

This typically indicates a problem with the Command Relay.

Resolution:

Check to be sure you have a Command Relay running. For more options, see the troubleshooting section for ["Command Relay / Delinea Platform Engine "](#) on the next page.

Active Policy Not Enforced

Issue:

The status of a policy is Active, but the policy is not being enforced.

Cause:

Policy changes can take up to 30 minutes to be enforced after a policy's status becomes Active or Inactive. This is caused by the agent internal caching.

Resolution:

If an active policy is not being enforced after 30 minutes, contact Delinea support.

Inactive Policy Still Seems Active

Issue:

A Login or Privilege Elevation policy status is Inactive, but you can still perform login or privilege elevation on the machine.

Cause:

Policy changes can take up to 30 minutes to be enforced after a policy's status becomes Active or Inactive. This is caused by the agent internal caching.

Resolution:

If an inactive policy is still in effect after 30 minutes, contact Delinea support.

Machine Not In Target List

Issue:

When setting up a PCS authentication policy, the Targets section is not showing the desired machine.

Resolution:

The targets you can select come from Inventory. If you are looking for a machine and it is not showing in the Targets list, check to see whether that same machine appears in the Inventory list.

If the machine not listed under Targets is also not listed under Inventory, run the discovery process. See ["Discovery"](#) on page 165.

If the machine not listed under Targets is listed under Inventory, contact Delinea support.

Command Relay / Delinea Platform Engine

This section gives solutions for issues related to Command Relay. The main technique for troubleshooting Command Relay is to look at the Command Relay logs.

Command Relay is one of the workloads deployed by the Delinea Platform Engine. The platform heavily depends on the Engine to run. Therefore, when troubleshooting Command Relay, it is also important to investigate potential problems with the Engine.

Increasing the Log File Detail Level

The default setting for Engine Pool logs includes critical errors only, without much detail. When you need detailed information, increase the verbosity of the default logging level to Debug in the Engine Pool's `appsettings.json` file. Edit this file:

```
C:\Program Files\Delinea Engine\<engine_version>\appsettings.json
```

Frequently Asked Questions

Question: Is Command Relay setting in Engine Pool for all engines under the same site?

Answer: Yes. You could create another site if you want to use a different domain.

Question: Why does Command Relay need the Active Directory (AD) domain admin credentials?

Answer: Command Relay uses the credentials to communicate with AD to store PCS policies. By default, AD users in the Domain Admins group have all the required permissions.

Question: What happens if I provide the wrong Active Directory domain admin credentials or if they expire?

Answer: Command Relay will stop working, and therefore no other Policy change will be applied. In the Command Relay log, you would see the following:

```

39 2024-02-01 06:59:22,052 [6] ERROR CommandRelay [(null)] - Failed to run workload
40 Delinea.CommandRelay.Common.VaultedDomainCredsException: Invalid domain creds (Logon
   Failure). Please check the Delinea Command Relay - Domain Account settings on the Engine/
   Site settings page, and make sure the account has domain administrative privileges to create
   the Delinea Zone.
41 ---> Delinea.CommandRelay.Common.LogonException: Invalid Domain Credentials. Logon user
   failed: Administrator, errorCode=1326
42 ---> System.ComponentModel.Win32Exception (1326): The user name or password is incorrect.
43 --- End of inner exception stack trace ---
44 at Delinea.CommandRelay.Common.RunAsProcess.Run(String cmd, String workDir) in
   D:\a\1\s\Delinea.CommandRelay.Common\RunAsProcess.cs:line 195
45 at Delinea.CommandRelay.Setup.RunLocalProcess(String cmd) in
   D:\a\1\s\CommandRelay\Setup.cs:line 287
46 at Delinea.CommandRelay.Setup.ValidateEnv() in D:\a\1\s\CommandRelay\Setup.cs:line 210
47 at Delinea.CommandRelay.DomainCredsHandler.ValidateCreds(CancellationTok stoppingToken)
   in D:\a\1\s\CommandRelay\DomainCreds.cs:line 64
48 --- End of inner exception stack trace ---
49 at Delinea.CommandRelay.DomainCredsHandler.ValidateCreds(CancellationTok stoppingToken)
   in D:\a\1\s\CommandRelay\DomainCreds.cs:line 82
50 at CommandRelay.TaskService.Initialize(HostClient client, CancellationTok
   stoppingToken) in D:\a\1\s\CommandRelay\TaskService.cs:line 235
51 at CommandRelay.TaskService.Run(HostClient client, CancellationTok stoppingToken) in
   D:\a\1\s\CommandRelay\TaskService.cs:line 54
52 at Delinea.CommandRelay.WorkloadWorker.ExecuteAsync(CancellationTok stoppingToken) in
   D:\a\1\s\CommandRelay\Workload.cs:line 66
53 Failed to run deployment: Command execution failed because the underlying process (
   CommandRelay.exe#2160) returned a non-zero exit code (3).
54

```

Command Relay Secret Stops Working

Issue:

The selected secret for Command Relay stopped working (service account).

Cause:

- This could happen if the selected secret is changed. For example, if you move the secret to a personal folder in Secret Server, it removes the EngineWorkload shared permissions on the secret, which causes permission failure in Command Relay.
- This could also happen if the underlying service account associated with this secret is changed; for example, password expired/not synced, account locked, AD permissions removed, and so on. Look at the failure log message for error details.

Command Relay Can't Log In

Issue:

Command Relay can't log in using the secret that works for the Secret Server Discovery service.

In the Command Relay log, you see that the Command Relay cannot log in:

```

2024-01-29 14:17:11,592 [10] INFO CommandRelay [(null)] - RunAsProcess info: domain=eric-sp-1.eric user=svc-
ssd

```

Privilege Control for Servers

2024-01-29 14:17:11,592 [10] INFO CommandRelay [(null)] - Normalized RunAs Info: user=svc-ssd domain=eric-sp-1.eric

2024-01-29 14:17:11,616 [10] ERROR CommandRelay [(null)] - Invalid Domain Credentials. Logon user failed: svc-ssd, errorCode=1385

2024-01-29 14:17:11,628 [10] ERROR CommandRelay [(null)] - Invalid domain creds detected, Exception=Delinea.CommandRelay.Common.LogonException: Invalid Domain Credentials. Logon user failed: svc-ssd, errorCode=1385

---> System.ComponentModel.Win32Exception (1385): Logon failure: the user has not been granted the requested log on type at this computer.

Resolution:

Fix the credentials.

IWA Doesn't Work When Installing Connector

Issue:

When trying to deploy Delinea Connector on a host, communication issues occur between the host and Integrated Windows Authentication (IWA). The host name also appears truncated wherever it appears in the Delinea Platform UI; for example, in the inventory and the list of engines.

Cause:

The host computer has a host name longer than the maximum Windows NetBIOS name length of 15 characters. The Powershell script supplied in ["Generating a Self-Signed Delinea Connector IWA Host Certificate" on page 509](#) for generating a certificate uses the truncated name, and therefore gets the wrong DNS name for the machine.

Resolution:

1. Rename the host computer with a name that is no more than 15 characters long.
2. Generate a new certificate for the host.
3. Remove the host from enrollment with IWA identity services.
4. Force removal of all data.
5. Re-enroll the host with the identity services provider using the new host name.

Secret Server

This section gives solutions for issues related to Secret Server.

Distributed Engine Not Working

Issue:

The Secret Server Distributed Engine is not working.

Resolution:

- Check to see whether the Engine has been Activated.
- Check the machine where the agent is running to be sure its Windows clock is correct.

Privilege Control for Servers Agent

This section gives solutions for issues related to the PCS Agent.

Increasing the Log File Detail Level

To turn on debugging for Linux agents, run the following commands as the root user:

- `/usr/share/centrifydc/bin/addebug set cloud.object TRACE`
- `/usr/share/centrifydc/bin/addebug on`

Logs are located in `/var/log/centrifydc.log`.

To turn off debugging, run the following command as the root user:

`/usr/share/centrifydc/bin/addebug off`

Turning On Debugging for SSHD

To turn on debugging for the sshd server:

Run `ps -ef | grep sshd` to find out whether you are using CentrifyDC-openssh or system stock sshd.

If you are using CentrifyDC-openssh:

1. Add `LogLevel DEBUG3` in the configuration file `/etc/centrifydc/ssh/sshd_config`.
2. Restart the server by running this command as the root user:

`systemctl restart centrify-sshd`

If you are using system stock sshd:

1. Add `LogLevel DEBUG3` in the configuration file `/etc/ssh/sshd_config`.
2. Restart the server by running this command as the root user:

`systemctl restart sshd`

Or, on Ubuntu/Debian:

`systemctl restart ssh`

Collecting Debugging Information

To collect debug info for the Delinea support team to investigate an issue:

1. Turn on debugging for Linux agent and sshd.
2. Reproduce the issue.
3. Run the following command as the root user:

`adinfo -t`

Provide the `/var/centrify/tmp/adinfo_support.tar.gz` file to the Delinea support team for their investigation.

Frequently Asked Questions

Question: My AD forest has multiple domains, so will each domain have a DelineaZone created?

Answer: No, there will be only one DelineaZone created in the forest when you deploy the very first Engine Pool in the forest.

Session Recording Stops Linux Agent Login

Issue:

Can not log in to Linux agent after enabling Session Recording in a Granular Privilege Elevation policy for Linux (see "Setting Up PCS" on page 601).

Cause:

The Linux agent requires Direct Audit to be enabled on the Agent when policies have session recording enabled.

Resolution:

Enable Direct Audit on the Linux agent by following the steps in "Step 10: Set Up Audit and Session Recording" on page 608.

AD User Can't Log In on Linux

Issue:

An AD user can't log in to a domain-joined Linux machine.

Resolution:

You will need a root shell for the following steps.

Suppose the user's AD user name is tom@acme.com.

- 1. Verify whether the AD user is visible on the Linux machine by running the following command in your root shell:

```
adquery user tom@acme.com
```

If the output is tom@acme.com is not a zone user, verify whether the Command Relay has successfully deployed the policy.

- 2. Verify whether the AD user has login permissions by running the following command in your root shell:

```
dzinfo --role tom@acme.com
```

Example output:

User: tom

Forced into restricted environment: No

MFA Service authentication: Supported

Privileged commands:

Name	Avail	Command	Source Roles
_____	_____	_____	_____
__pe_sys_6240d333-6256-4221-9a23-39bfc381202c/DelineaZone	No	*	Mansion-Grove-Elevation/DelineaZone
__pe_6240d333-6	No	*	Mansion-Grove-Elevat


```
256-4221-9a23-3
9bfc381202c/DelineaZone
ineazone
...
...
```

- 3. If you don't see Password Login and Non password Login in the Effective rights, verify whether the Command Relay has successfully deployed the policy.
- 4. It can take up to 30 minutes before the Linux agent refreshes the latest authentication and authorization information from AD after the policy deployment. To force a refresh, you can run:
`adflush -f`
- 5. If the `adquery` and `dzinfo` commands show the expected result, contact Delinea support. Provide the information described in "Collecting Debugging Information" on page 665.

AD User Can't Run dzdo on Linux

Issue:

An AD user can't run `dzdo` commands on a domain-joined Linux machine.

Resolution:

You will need a root shell for the following steps.

Suppose the user's AD user name is `tom@acme.com`.

- 1. Verify whether the AD user has privileged command rights by running the following command in your root shell:

```
dzinfo --commands tom@acme.com
```

Example output:

User: tom

Forced into restricted environment: No

MFA Service authentication: Supported

Privileged commands:

Name	Avail	Command	Source Roles
-----	-----	-----	-----
__pe_sys_6240d333-6256-4221-9a23-39bfc381202c/DelineaZone	No	*	Mansion-Grove-Elevation/DelineaZone
__pe_6240d333-6256-4221-9a23-39bfc381202c/DelineaZone	No	*	Mansion-Grove-Elevation/DelineaZone

...

...

2. If you don't see anything in `Privileged` commands, verify whether the Command Relay has successfully deployed the policy.
3. It can take up to 30 minutes before the Linux agent refreshes the latest authentication and authorization information from AD after the policy deployment. To force a refresh, you can run:
`adflush -f`
4. If the Connector appears Active at **Settings > Connectors** but you see the error message `unable to communicate with the Delinea Platform`, you can ignore the message.
5. If the `dzinfo` command shows the expected result, contact Delinea support. Provide the information described in ["Collecting Debugging Information"](#) on page 665.

Useful Commands and Tips for AD Client on *.nix

This section provides suggestions for commands and techniques you can use to help troubleshoot issues with Active Directory on machines that run on UNIX, Linux, or another supported operating system derived from UNIX/Linux.

Looking Up Basic Information

(For *.nix only)

- To check the general status of the client:
`$ adinfo`
- To see the current domain controller the client is using:
`$ adinfo --server`
- To see the current domain the agent is joined to:
`$ adinfo --domain`
- To see whether the agent is connected to AD or in offline mode:
`$ adinfo --mode`
- To see the version of the installed client:
`$ adinfo --version`
- To see the corresponding Delinea PCS version:
`$ adinfo --suite-version`
- To view Active Directory connectivity to the current domain:
`$ adinfo --test`
- To view the current Active Directory site:
`$ adinfo --site`
- To see the current joined Delinea zone:
`$ adinfo --zone`

Or, in distinguishedName format:

```
$ adinfo --zonedn
```

More Detailed Troubleshooting Information

(For *nix only)

This section describes how to get specialized or more-detailed information to help troubleshoot issues.

DNS

- To check for the "joined-as" name (the local host name and joined-as name might be different):

```
$ adinfo --name
```

- To check the status of the DNS cache and stats:

```
$ adinfo --diag dns
```

Connectivity

- To check connectivity with an AD domain:

```
$ adinfo --test [domain.name]
```

- To check network connectivity statistics:

```
$ adinfo --sysinfo neststate
```

- To test connectivity with a specific domain controller:

```
$ adinfo --T --servername [domain.controller.name]
```

Active Directory

- To see the current AD Global Catalog:

```
$ adinfo --gc
```

- To see the domain/forest map:

```
$ adinfo --sysinfo domain
```

- To see the status of the AD computer trust relationship:

```
$ adinfo --sysinfo adagent
```

Configuration

- To parse the contents of the `centrify.conf` file:

```
$ adinfo --config
```

- To show the client's in-memory configuration parameters:

```
$ adinfo --sysinfo config
```

Microsoft Kerberos

- To view Kerberos information like supported encryption types, key version and registered SPNs:

```
$ adinfo --computer
```

- **PKI: adcert** - Delinea Microsoft PKI client

Auto-Enrolling PKI Certificates

(For *nix only)

Auto-enrolling computer PKI Certificates requires eligible template and communications. Use one of the following techniques.

- Using the computer object to authenticate:

```
$ dzdo /usr/share/centrifydc/sbin/adcert --enroll --machine
```
- Using a user to authenticate (substitute the user name for [ADusername]):

```
$ dzo /usr/share/centrifydc/sbin/adcert --enroll --user [ADusername]
```

To test a user's password:

1. Run the following command (substitute the user name for [username]):

```
$ adinfo -A --user [username] #
```
2. When prompted, enter the user's password. Expected output:

```
Password for user "username" is correct
```

Dynamic DNS

(For *nix only)

This section shows some useful commands using **addns**, a dynamic DNS client for AD DNS or RFC 2136-compliant servers.

- To renew DNS using machine credentials:

```
$ sudo addns --update --machine
```
- To renew DNS using user credentials:

```
$ sudo addns --update --user [ADusername]
```
- To renew DNS only on a specific interface (for example, eth0):

```
$ sudo addns --update --machine --interface eth0
```

Querying AD Users and Groups

(For *nix only)

This section shows some useful commands using **adquery**, which provides information about Active Directory users and groups that are UNIX-enabled by Delinea Platform.

- To view all UNIX-enabled users:

```
$ adquery user
```

In Express mode, this command shows all AD users. In Zone mode, it shows only authorized users.
- To view all UNIX-enabled groups:

Privilege Control for Servers

```
$ adquery group
```

In Express mode, this command shows all AD groups. In Zone mode, it shows only UNIX-enabled groups.

- To view a user's entry in UNIX passwd file style:

```
$ adquery user [username]
```

- To view a group entry in UNIX group file style:

```
$ adquery group [groupname]
```

- To view only the user or group's AD group memberships:

```
$ adquery user [user] --adgroup
```

- To view all information about a user or group, including AD object attributes:

```
$ adquery user|group [user or group] -A
```

- To view the distinguished name of a user or group:

```
$ adquery user|group [user or group] --dn
```

- To view all information and include password expiration, account lockout/enabled state:

```
$ sudo adquery user [user] -A
```

- To view information about a computer:

```
$ adquery user [computername]$ -A
```

- To get results from cache instead of fetching from AD:

```
$ adquery user|group [options] --cache-first
```

Delinea Cache Commands

(For *nix only)

This section shows some useful commands using **adflush**, which clears the Delinea cache in the local computer (dc, gc, credential, and dns).

- To flush the authorization cache:

```
$ dzdo adflush --auth
```

- To rebind and force a new DC selection:

```
$ dzdo adflush --bindings
```


- To flush the DNS cache:

```
$ dzdo adflush --dns
```

- To expire the information from domain controllers and global catalogs:

```
$ dzdo adflush --expire
```

- To force complete removal/expiration even when disconnected:

 Use this command with care.

Privilege Control for Servers

```
$ dzdo adflush --force
```

- To refresh the `krb5.conf` file:

```
$ dzdo adflush --trusts
```

- To clear the health history:

```
$ dzdo adflush --health
```

- To clear the cloud connectors (when MFA is being used):

```
$ dzdo adflush --connectors
```

Group Policy Commands

(For *nix only)

This section shows some useful commands related to group policies.

The following commands use **adgpupdate**, which triggers the group policy refresh interval.

- To refresh the GPOs in the system:

```
$ adgpupdate
```

- To refresh only computer GPOs:

```
$ adgpupdate --target Computer
```

- To refresh only user GPOs:

```
$ adgpupdate --target User
```

The following commands use **adgpresult** to view an RSoP (resultant set of policy) report for the local system or user.

- To view the report for computer and user:

```
$ adgpresult
```

- To view the report for the computer:

```
$ adgpresult --computer
```

- To view the report for the current user:

```
$ adgpresult --user
```

- To view the report for a particular user:

```
$ dzdo adgpresult --user [user.name]
```

Joining Active Directory (adjoin)

(For *nix only)

This section shows some useful commands using **adjoin**, which joins an Active Directory domain.

To run `adjoin`, you need the following:

Privilege Control for Servers

- Permission level of root or sudo
- Credentials (or the keytab) of an AD user that can join computers to a container (not the Domain Admin user)
- Distinguished Name of the container that you will place the system in AD; for example, "ou=servers,ou=unix"
- Domain name of the domain you are joining
- Clear network path to the AD domain controller (DC) or DCs you are using (dns, global catalog, kerberos, ldap, cifs, ntp)

Following are some useful ways to use `adjoin`:

- To join AD in workstation/express mode (AD user must be able to add computers to "ou=workstations,ou=unix"):

```
$ sudo adjoin --workstation --container "ou=workstations,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```
- To join AD in Self-Service mode (before running this command, the AD/Delinea administrator must create the machine ahead of time using Access Manager or Delinea Powershell cmdlets):

```
$ sudo adjoin --selfserve [domain.name]
```
- To join AD in zone mode (for example, Global zone):

```
$ sudo adjoin --zone Global --container "ou=servers,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```
- To join AD in zone mode and don't initialize (precache):

```
$ sudo adjoin --noinit --zone Global --container "ou=servers,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```
- To join AD and trust the computer for delegation:



Use this command only if you have the expertise. This command has security implications.

```
$ sudo adjoin --trust Global --container "ou=servers,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```

- To join AD in workstation mode and specify a workstation license:

```
$ sudo adjoin --licensetype "workstation"--workstation --container "ou=workstations,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```
- To use a specific domain controller to join (for example, dc1.hq.fabrikam.com):

```
$ sudo adjoin --server dc1.hq.fabrikam.com Global --container "ou=servers,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```
- To join a Mac in workstation mode and instruct Delinea to use the Apple algorithm to generate UID/GID scheme:

```
$ sudo adjoin --enableAppleIDGenScheme --container "ou=macs,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```
- To join AD and provide a different AD name than the local system name (for example, adserver rather than localhost):

```
$ sudo adjoin --name adserver --container "ou=servers,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]
```

- To join AD using keytab (kinit Authorized AD user keytab first, then run adjoin without the --user option):

```
$ env KRB5_CONFIG=[/path/to/krb5.conf] /usr/share/centrifydc/kerberos/bin/kinit -kt  
/path/to/keytab [principal]:
```

```
$ sudo adjoin --zone Global --container "ou=servers,ou=unix" --verbose [domain.name]
```

What Happens When adjoin Runs Successfully

When adjoin runs successfully, it activates the DirectControl agent (adclient/ DelineaDC service), with the following effects:

1. Creates a computer object in AD and sets SPNs for http, host, nfs, cifs, afpserver.
2. Establishes a secure communication channel between the system and Active Directory.
3. A forest/domain/site map is created to locate the nearest DCs.
4. The Kerberos environment (krb5.conf, krb5.keytab) are maintained by Delinea (configurable). A backup is created.
5. Network time is synchronized with AD DCs (configurable).
6. The PAM (Pluggable Authentication Modules) are modified to include Delinea auth, account, password, and session modules. A backup of the previous configuration is made.
7. The NSS (Name Service Switch) providers for users and groups defaults to AD first, then other methods (such as files, ldap, and so on). A backup of the previous configuration is made. In the OS X platform, the PAM/NSS functions are channeled using the Directory Services Plugin API.
8. An Access Control Model is enforced depending on the zone mode:
 - In zone mode, authorization (RBAC) follows zone rules: defaults to closed, only authorized users can access, and enabled groups are visible.
 - In express/workstation mode, only authentication is facilitated. The system is open for all AD users, and all groups are visible.
9. Privilege Elevation: Delinea-enhanced sudo (dzdo) becomes active based on the roles and rights defined.
10. User and Group identity (RFC2307) data in AD is stored within the Delinea zone, not with the user or group object.
11. The virtual registry is initialized, and group policies are enforced.

Leaving Active Directory (adleave)

(For *nix only)

This section shows some useful commands using **adleave**, which leaves an Active Directory domain.

To run adleave, you need the following:

- Permission level of root or sudo
- For the online leave command, authorized AD user credentials

Following are some useful ways to use adleave:

Privilege Control for Servers

- Leave the domain and disable the computer object (orphan object left behind):
`$ dzdo adleave --user [Authorized ADUsername]`
- Leave the domain and remove computer object (frees license):
`$ dzdo adleave --user [Authorized ADUsername] --remove`
- Offline/forced leave (no AD connectivity required, must clean up in AD):
`$ dzdo adleave --force`

What Happens When adleave Runs Successfully

When `adleave` runs successfully, it has the following effects, some of which depend on how the command was run:

- Online with the `--remove` object: The object in AD is removed from the container and from the zone (frees license).
- Online without the `--remove` object: The object in AD is marked as disabled. Must be overwritten to rejoin.
- Offline: The object in AD is left orphaned. Cleanup must happen through any Delinea API (AM, PowerShell, `adedit`).
- The UNIX environment is reset and rolled back (Kerberos, PAM, NSS).
- The Delinea `adclient` (DelineaDC) service is disabled.

Privilege Elevation ("dz" commands):

(For *nix only)

This section shows some useful commands using **`dzinfo`**, which displays information about the user's access controls.

- To view self access (all):
`$ dzinfo`
- To view the properties of the role(s), including effectiveness:
`$ dzinfo --roles`
- To view how you can access the system (PAM rights):
`$ dzinfo --pam`
- To view the commands you can run:
`$ dzinfo --commands`
- To view the computer roles that apply to the system (requires privilege elevation):
`$ dzinfo --computer-role`
- To view authorization information about another user (requires privilege elevation):
`$ dzdo dzinfo [user.name]`
- To test a command against the role:
`$ dzinfo --test [path/to/binary] [options]`

Delinea-enhanced sudo (dzdo)

(For *nix only)

The dzdo command is a Delinea-enhanced version of the sudo command that uses Delinea zone data in AD for commands. In all other ways, it is identical to sudo.

To view version information (as of 2015, based on sudo 1.8.10p3):

```
$ dzdo -v
```

DirectAudit Commands ("da" commands)

(For *nix only)

This section shows some useful DirectAudit commands.

The following commands use **dainfo**, which shows information about the status of the audit agent.

- To view the audit agent status:
\$ dainfo
- To view status with verbose output:
\$ dainfo --diag (or dadiag)
- To view contents of the configuration file:
\$ dainfo --config
- To view audited status of another user (requires privilege elevation):
\$ dzdo dainfo --username lisa.simpson

The following commands use **dacontrol**, which controls the status/configuration of the DirectAudit client (requires privilege elevation).

- To set the installation (if not set by Group Policy):
\$ dzdo dacontrol --installation [installation-name]
- To check if the audit agent is enabled:
\$ dzdo dacontrol --query
- To enable direct audit:
\$ dzdo dacontrol --enable
- To disable direct audit:
\$ dzdo dacontrol --disable

Important Files and Folders

(For *nix only)

This section lists some important files and folders that you should be familiar with to successfully run and troubleshoot PCS and the Delinea Platform on UNIX/Linux.

- In the directory `/usr/share/centrifydc/` (or OS X El Capitan and later, `/usr/local/share/centrifydc`):
 - `bin`
Contains user binaries, including Delinea-enhanced `openldap` tools like `ldapsearch`
 - `sbin`
Contains system binaries, including `adcert` and Delinea-enhanced `OpenSSH`
 - `samples`
Sample files for `hadoop`, `adedit` and local account management
- In the directory `/etc/centrifydc`:
 - `centrifydc`
Configuration files for the `DirectControl` agent
 - `centrifyda`
Configuration files for the `DirectAudit` agent
 - `centrifycc`
Configuration files for the `Privilege Service CLI Toolkit for AAPM`
 - `openldap`
Configuration files for Delinea-enhanced `OpenLDAP` proxy, if installed
 - `ssh`
Configuration files for Delinea-enhanced `OpenSSH`s
- In the directory `/var/centrifydc`:
 - `kset*` files
Dynamic information about the environment
 - `reg`
Virtual registry which contains the computer and user hives (user GPO disabled on Servers)
- In the directory `/var/centrify`:
 - `net/certs`
Location of any Microsoft Certificate Authority auto-enrolled certificates, keys, and trust chain

ITP and PCCE

The Delinea Platform offers capabilities of Cloud Infrastructure Entitlement Management (CIEM) and Identity Threat Detection and Response (ITDR) in a seamless experience unified with your secrets vault and other privileged access management capabilities.

Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE) help to increase the security of your organization against the modern threats of identity-based attacks and over-privileged access to cloud infrastructure and SaaS tools.

A subset of these capabilities is included in Continuous Identity Discovery (CID), which extends Secret Server Cloud on the Delinea Platform, enabling enhanced discovery of privileged accounts within cloud environments. To learn more, see "Continuous Identity Discovery" on page 738.



Note: Throughout this documentation on ITP/PCCE, the terms **users**, **accounts**, and **identities** generally refer to cloud service users and accounts or cloud identities, and not to Delinea Platform users.

Identity Threat Protection

ITP helps increase security from identity-based threats such as malicious insiders, account takeovers, and privilege escalations, ensuring that risks and threats are discovered, investigated, and mitigated in line with security operations.

ITP enables:

- **Least Privilege and Secure Access Baseline:** Restrict privileges to Just Enough Access, thereby detecting and eliminating risks of stale access, over-privileges, and privilege escalation paths across cloud services and applications.
- **Lifecycle Change Monitoring:** Eliminate privilege sprawl and incomplete off-boarding by continuously monitoring identity, access, and usage data to ensure that employees and external contractors do not hold access privileges they no longer require.
- **Automate Remediation and Incident Response:** Provide automated remediation and response workflows to ensure that risks are eliminated and threats are mitigated through easy integrations with SIEM, SOAR, and XDR solutions to ensure standard procedures in handling identity and access incidents.

Privilege Control for Cloud Entitlements

Privilege Control for Cloud Entitlements (PCCE) reduces access risks across multi-cloud infrastructure by controlling privilege sprawl. The benefits of PCCE include:

- **Right Sizing Permissions to Prevent Privilege Escalations:** Mitigate complex access risks from human and machine identities, including third parties, across cloud infrastructure, applications, and IAM solutions.
- **Hardening the Identity Security Posture:** Automatically monitor IaaS, SaaS, and IAM solutions to identify misconfigurations and exposed resources, ensuring continuous compliance with standards and industry regulations.
- **Establishing a Secure Access Baseline with Advanced Analytics:** Maintain Least Privilege by eliminating risky and excessive access with ML-based contextual insights and remediating misconfigurations across cloud environments.

Setting Up ITP and PCCE

For instructions on setting up ITP and PCCE, see the following topics:

- [Integrating AWS with the Delinea Platform \(PCCE\)](#)
 - [Integrating Individual AWS Accounts \(via CloudFormation\)](#)
 - [Integrating Multiple AWS Accounts \(via CloudFormation StackSets\)](#)
 - [Integrating Individual AWS Accounts via Third-Party Tools](#)
 - [Integrating AWS Identity Center with the Delinea Platform \(PCCE\)](#)
- [Integrating Entra ID & Azure Cloud with the Delinea Platform \(ITP/PCCE\)](#)
- [Integrating Google Cloud Platform \(GCP\) with the Delinea Platform \(ITP\)](#)
- [Integrating Okta with Delinea Platform \(ITP\)](#)
- [Integrating PingOne with Delinea Platform \(ITP\)](#)
- [Integrating Snowflake with Delinea Platform \(ITP\)](#)
- [Integrating Workday with the Delinea Platform \(ITP\)](#)

Learn more about Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE):

- [ITP/PCCE Assets](#)
- [Recurring Reports](#)
- [Identity Posture](#)
- [Threat Center](#)
- [Configuring Risk](#)
- "Continuous Identity Discovery" on page 738

ITP/PCCE Inventory

For both Identity Threat Protection and Privilege Control for Cloud Entitlements, Inventory pages provide a centralized and comprehensive view of all identities, access privileges, assets, and activities across an organization's cloud services and applications. This visibility is essential for detecting and mitigating identity risks and active threats, ensuring compliance, and maintaining a secure access baseline.

Inventories enable organizations to:

- **Detect and Eliminate Over-Privileges:** By having a detailed inventory of access privileges, organizations can identify and mitigate over-privileges based on granular usage data and AI-based recommendations.
- **Monitor for Misconfigurations and Exposed Resources:** Inventories help in detecting risky misconfigurations such as exposed Git repositories and stale file access on shared drives, thereby hardening the identity security posture.

You can use inventories to do the following:

- Gain a holistic view of all the connected applications, their users, and access.
- Identify important issues across your organization like stale cloud service accounts and users without MFA.
- Define Collections that can later be reused for other product features such as security rules and reports.

The inventory pages display information that was either gathered from integrated systems or entered manually and then processed.

Inventory Types

ITP/PCCE inventories are displayed on the following pages:

- **Identities**: Displays identities and accounts.
 - **Identity**: A unique identity (human or nonhuman) that owns one or more cloud service accounts. A nonhuman identity could be a machine identity, an automatic identity, or any other identity that doesn't belong to a human.
 - **Account**: A unique account (human or nonhuman) in a single application. A nonhuman account might be a service account, a workload, or even a user account that is used for automated tasks.
- **Groups**: Displays entities that define permissions granted to multiple accounts. This could be an IdP group (like a group of engineers who use the same design tools to build their product or application) or an AWS role that grants the same permissions to similar actors. The Groups table displays the applications in which the groups are managed, not the applications to which those groups grant access.
- **Assets**: Displays every object in integrated systems to which users can be granted access, like files, folders, databases, virtual machines, and applications.
- **Memberships**: Displays all groups and their members. For example, if a group represents the Engineering department, the Membership inventory presents all its members. You can use this page to find the relationship between groups and their members, such as all groups a specific person belongs to.
- **Access Policies**: Displays effective access and effective permissions. Effective access represents the permissions an entity (for example, a user) has on another entity (for example, an asset), based on what access was granted. Effective permissions are the combination of direct and indirect permissions used when accessing an object. You can use this page to find the relationship between an entity (cloud service user or group) and an asset.
- **Privileges**: Displays a list of all privileges at all levels.
- **Activities**: Shows actions taken by various identities, and when each action was done.

Inventories User Interface

To access inventories, click **Inventory** from the left navigation menu of the Delinea Platform. Select one of the choices from the secondary menu, such as Identities.

Identities

AWS Users

Enabled/Unknown Status Users

Group By

Showing 51,073 Identities

Columns

Identities

Accounts

<input type="checkbox"/> Identity	Source Apps	Access To Apps	Incidents ↓	Tags
<input type="checkbox"/> Taylor Watts			8	-
<input type="checkbox"/> Crystal Lewis			8	-
<input type="checkbox"/> Shannon Leon...			8	-

Searching by Custom Properties

You can search by custom application properties, such as subscriptions in Azure or public repositories in GitHub or GitLab. This enables you to better scope the results based on your unique organizational values.

Custom properties are added by:

- **The Delinea Platform:** Each built-in integration exposes a set of custom properties. While custom properties retain the naming from their source, some imported properties are normalized on the platform with standard names.
- **Users:** You can add custom properties (when building a custom integration) that enable you to import and search by any property from the source application.

Sorting the Inventory Table

Each inventory table has a default sort order, indicated by the dark arrow displayed in the column header:

Identity ↑	Source Apps	Access To Apps	Incidents ↑
Current sort			Potential sort

To change the sort order, hover the pointer over a column header. When a dimmer arrow is displayed, you can click it to change the sort order.

Using Other Views

In addition to the Inventory table, most inventory items also have a single-entity view and a quick view.

Single-Entity View

To see more information about an inventory item, open its single-entity view by clicking either the entity name (leftmost table column) or the target name (in Access Policies, Membership, and Activities tables).

The single-entity view shows much more information about the inventory entity; for example, top incidents and MITRE tactics. You can investigate further using the Access Explorer.

Quick View

When you hover over the entity name, a quick view is displayed. The quick view shows a short list of commonly needed information. You can also investigate in the Access Explorer, show the entity in the source app (in some cases), and show the single-entity view.

Configuring Table Columns

You can customize the presentation of tables in the following ways:

- Choose which columns are displayed
- Resize the column widths
- Change the order of the columns

These options are available in all inventory tables. Your choices are relevant to the specific page where you made the choices and will persist through future login sessions.

To set the displayed columns:

1. From an inventory table, click **Columns** above the table. The list of available columns is displayed.
2. To display a column, select it. To hide a column, clear its selection. The column display adjusts immediately. If a column name is dimmed, it cannot be hidden.

To set the column width:

1. From an inventory table, point the cursor between column headings where you want to adjust the width until the cursor changes to multiple arrows.
2. Drag the cursor left or right to adjust the column width.

To set the column order:

1. From an inventory table, point the cursor at a column you wish to move. The gray column dividers on both sides are displayed.
2. Drag and drop the column to its new position.

Exporting a Table as CSV

You can download a file in CSV format containing all information displayed on an inventory page. If the download is limited to a certain number of entries, that limit is displayed when hovering over the download icon. To download more entries than the limit allows, filter the table to sets with fewer than the maximum number of entries, then download each set separately.

Using Tags

Tags are descriptive keywords (metadata) attached to data so you can find the data by browsing or searching. Tags are displayed in inventory tables and in the single-entity view. To get more information about any system tag, hover your cursor over the tag to read an explanation.

When an application is integrated with the platform, entities tagged in the source system are similarly tagged in the platform. In some cases, the platform also applies its own tags.

You can apply tags manually from most inventory pages (except the Membership and Access Policies pages) or from the single-entity view. You can apply existing tags or create new tags. You can apply tags to one or multiple entities simultaneously.

To apply existing tags in an inventory page:

1. Select the row you want to tag.
To apply the same tag to multiple rows, select multiple rows.
2. Click **Add Tags**, then click **Add tags** again.
3. To apply an existing tag, select the tag, then click **Save**.
You can search for tags by typing the first few letters.

To create and (optionally) apply new tags in an inventory page:

1. Select an inventory row.
If you intend to apply your new tag at the same time you create it, select one or more rows.
2. Click **Add Tags**, then click **Add tags** again.
3. Type a new tag name.
4. Click **Add New**.
5. (Optional) To apply the new tag, click **Save**.
If you do not apply the tag, the new tag is still created. It can be applied to entities later. You can apply both existing and new tags in the same step.
6. To add more new tags, type another new tag name and click **Add New**.

Filtering an Inventory Table

By default, each inventory page includes a table displaying all data relevant to the page. You can filter the table to show only the data you are interested in, creating granular queries to understand the inventories, groups, and assets in your Delinea Platform environment. For example, you can display all the identities with admin privileges whose cloud service accounts were disabled or suspended (or are unknown).

For more information about how to use basic and advanced filtering, see ["Filtering in List Pages"](#) on page 48.

For more information about the filter fields for each inventory, see ["Inventory Filter Properties"](#) below.

Inventory Filter Properties

This section is a reference to all the filter properties provided by the Delinea Platform in the Inventory pages.

Identities

Category	Property	Description
Account	Access To Apps	The applications a cloud service user (or service account) can access. The access might be direct or indirect (such as federated access).
	Admin Access	Cloud service user accounts with administrative privileges. You can specify the application for which you want to find users with admin access. To modify this setting, select Settings > Authorization Configuration .
	Blast Radius Risk	Impact of an account to be taken over, based on the account's access and type of access.
	Email	Email of the cloud service user (or service account) as found in the application.
	First Name	First name of the cloud service user (or service account) in an application. The First Name may vary from application to application.
	ID	ID
	Incidents Count	The number of incidents an account has (for example, the incidents in the AWS account).
	Is External	Find accounts that are external (or not external). External accounts are based on the email and properties of the account being different from internal users (or as stated in the downstream application).
	Is Managed	A managed account is managed by the current system's administrator. Use this filter to find all accounts your administrators have full control over, or those they do not control that have access to your systems.
	Is MFA Enabled	Find applications where MFA is set (or not set). MFA settings may be different in different accounts; for example, MFA might be enabled in Okta but disabled in Slack.
	Last Login At	Date of the last login in a specific application.
	Last Name	Last name of the cloud service user or service account. The Last Name may vary from application to application.

Category	Property	Description
	Overall Risk	The overall risk is calculated based on the probability that an account can be taken over and the blast radius risk (defined earlier in this table).
	Detection Rule Name	Cloud service users who match a specific detection rule; for example, finding all the users that matched the brute force attack.
	Privileged Access	Cloud service user accounts with privileged access. You can select the application to identify users with privileged access. To modify this configuration, select Settings > Authorization Configuration .
	Shadow Admin Access	Cloud service user accounts with shadow-admin privileges across various applications. You can choose the specific application for which you want to find users with shadow-admin permissions. Shadow-admin permissions grant users administrative capabilities with a reduced set of permissions they currently possess.
	Source App	The application in which the account is a registered cloud service user. For example, if a user has federated access to AWS through an IDP (such as Okta), Okta is the source app, and AWS is found in the Access to app filter.
	Status	The status of the account in the source application, such as Deleted, Disabled, Enabled, or Unknown.
	Sub Type	All the available sub-types of non-human Identities.
	Tags	Tags that are associated with the account (such as Admin, Privileged Access). Tags are created automatically by the AI engine, manually by the end user, or are based on tags in the source system.
	Take Over Risk	The probability that an account will be taken over by an external identity.
	Type	User or Service Account
Collection	Name	The named Collection is used as a filter. All collection types can appear in the filter. If an Access-type collection is used, then the identities that matched will be returned.

Category	Property	Description
Identity	Blast Radius Risk	Identities are filtered based on the risk imposed by their access collection. This filter focuses on the highest Blast Radius among all related accounts, providing insights into the extent of potential damage in case of a security breach. With this filter, you can quickly locate critical accounts or high-risk cloud service users with extensive access permissions. Use this filter to prioritize security measures and reduce the overall risk of breaches.
	Department	The department in which the identity works (for example, Customer Support, Sales, HR).
	First Name	The first name of the identity. Taken from the primary account of the identity, which is often the HR system or the IdP.
	Hired At	Date hired.
	Last Name	The last name of the identity. Taken from the identity's primary account, which is often the HR system or the IdP.
	Manager	The name of the identity's manager.
	Name	The name of the identity, which is either taken directly from the primary account of the identity (the HR system or IdP in most cases) or a combination of the First and Last names from the Primary account.
	Overall Risk	Comprehensive risk of an identity, considering the combined risks of its individual accounts. Incorporates two main components: Account Takeover Risk, which gauges the vulnerability of the identity to unauthorized access, and Blast Radius, representing the highest scope of permission the identity can achieve. Use this filter to search for identities with significant security concerns, prioritizing measures to mitigate potential breaches and safeguard sensitive data.
	Source Apps	All applications for which the identity has a registered user account. For example, if a user has federated access to AWS through an IdP (such as Okta), only Okta will be represented as the source app, and AWS will be in the Access to App filter.
	Tags	Tags associated with the identity (such as Senior Employee, Involved in Credential Leak, Finance Employee). Tags are created automatically by the AI engine or manually.

Category	Property	Description
	Take Over Risk	The ease with which an attacker could gain access to any of an identity's connected accounts. This filter assesses the risk level posed by each individual account, providing a comprehensive understanding of the identity's overall security vulnerability. By utilizing this filter, you can identify identities with weak account security, so you can prioritize security enhancements and protect against potential unauthorized access and data breaches.
	Terminated At	Terminated At
	Title	The job title of the identity (such as CTO, Software Engineer).

Groups

Category	Property	Description
Group	Admin Access	User accounts with administrative privileges. You can specify the application for which you want to find users with admin access. To modify this setting, select Settings > Authorization Configuration.
	Alternative Name	The alternative name of the group is presented to users and reviewers across the platform alongside the group name and is used to provide a clearer name for of the group
	Collections	The named Collection is used as a filter. Filtering is based upon the results of the Collection query in this inventory. The filter result shows all the groups that matched the Collection.
	ID	ID
	Incidents Counts	The named Collection is used as a filter. Filtering is based upon the results of the Collection query in this inventory. The filter result shows all the groups that matched the Collection.
	Is Empty	Empty groups or non-empty groups.
	Name	The name of the group as stated in the source system.
	Origin Type	The type of the group in the source application (such as AWS Role or Salesforce Profile).
	Owner	The name of the owner of the group, if any.

Category	Property	Description
	Detection Rule Name	Filter based on groups that matched a specific detection rule. For example, find groups that grant admin access.
	Privileged Access	User accounts with privileged access. You can select the application to identify users with privileged access. To modify this configuration, select Settings > Authorization Configuration .
	Shadow Admin Access	User accounts with shadow-admin privileges across various applications. You can choose the specific application for which you want to find users with shadow-admin permissions. Shadow-admin permissions grant users administrative capabilities with a reduced set of permissions they currently possess.
	Source App	The app on which the group is managed.
	Tags	Tags associated with the group (for example general, birthright group). Tags are created automatically by the AI engine, manually, or are based on the tags in the source system.

Assets

Category	Property	Description
Asset	Created At	Creation date of the asset, if available.
	Collections	The named Collection is used as a filter. Filtering is based upon the results of the Collection query in this inventory. The filter result shows all the Assets that matched the Collection.
	ID	ID
	Incidents Counts	The number of incidents associated with the asset.
	Last Used At	The last time the asset was used (accessed, modified, deleted or created). This data is available mainly for Secrets and Applications, and is not available in most other asset types.
	Name	Name of the asset.
	Origin Type	The type of the asset on the source application (for example: EC2 machine in AWS, or Application in Okta).
	Detection Rule Name	Filter based on assets that matched a specific detection rule. For example, find production assets that can be accessed by non-admins.

Category	Property	Description
	Source App	The app on which the asset is managed.
	Tags	Tags associated with the asset (for example, Production or Test Environment).
	Type	Assets are "normalized" (grouped) to a minimal set of types across all applications. Assets can therefore be filtered by their "normalized" Type (such as Virtual Machine), and they can be filtered specifically by the name of the asset in the source system (for example, EC2 machines on AWS).

Memberships

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities - Account	See "Identities" on page 684.
	Identity	Collection	Same as Identities-Collection	See "Identities" on page 684.
	Identity	Identity	Same as Identities - Identity	See "Identities" on page 684.
	Group	Group	Same as Groups inventory	
Target	Group	Group	Same as Groups inventory	
Access		Membership	Added at	Date when this membership was created.
			Added by	Person who created this membership.
			Direct Access	Direct Access
			Collections	Collections

Access Policies

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities -Account	See "Identities" on page 684.
	Identity	Collection	Same as Identities -Collection	See "Identities" on page 684.
	Identity	Identity	Same as Identities -Identity	See "Identities" on page 684.
	Group	Group	Same as Groups	
Target	Asset	Asset	Created At	Creation date of the asset, if available.
			Collections	The named Collection is used as a filter. Filtering is based on the results of the Collection query in this inventory, so the results will be all the Assets that matched the Collection.
			ID	ID
			Incidents Count	The number of incidents associated with the asset.
			Last Used At	The last time the asset was used (accessed, modified, deleted or created). This data is available mainly Secret or Applications assets, and is not available in most other asset types.
			Name	Name of the asset.
			Origin Type	The type of the asset on the source application (for example: EC2 machine in AWS, or Application in Okta).
			Detection Rule Name	Filter based on assets that matched a specific detection rule. For example, find production assets that can be accessed by non-admins.
			Source App	The app on which the asset is managed.

Filter	Entity Type	Category	Property	Description
			Tags	Tags associated with the asset (for example, Production or Test Environment).
			Type	Assets are "normalized" (grouped) to a minimal set of types across all applications. Assets can therefore be filtered by their "normalized" Type (such as Virtual Machine), and they can be filtered specifically by the name of the asset in the source system (for example, EC2 machines on AWS).
Access		Access	Collections	The named Collection is used as a filter. Only Access Collections will yield results in this inventory.
			Granted at	Date when the access policy was created.
			Granted by	Person who created the access policy.
			Is Direct	A direct assignment of access is any access granted to the account/group directly and not through another group. When marked as Yes, only direct access will be shown and calculated in the result. When marked as No, not only indirect will be included. To include both options, do not use this filter.
			Last Used At	Date when the access policy was most recently used.
			Limit Inheritance	Include only the first asset in the system that matches the query. Does not return any inherited assets. For example, if you want to find administrative access in a file system, and a user has access to a folder that contains a file, this filter returns only the folder.

Filter	Entity Type	Category	Property	Description
		Privilege	Is Role	Privileges of a role on different assets. Different users get the same privilege (through the same role), but on different assets. In the platform, this is called a local role.

Privileges

Category	Property	Description
Privilege	Child Privileges	Privilege that contains a specific child privilege. For example, search the privilege Add MFA and find every admin or similar role that can add MFA devices.
	Is Role	Filter on whether privilege represents a role on the application.
	Origin Name	The name of the privilege in the source application.
	Source App	The app on which the privilege is managed.
	Tags	Tags associated with the privilege (for example, Production or Test Environment).
	Type	Privileges are "normalized" (grouped) to a minimal set of types across all applications. Privileges can therefore be filtered by their "normalized" Type (such as Administrative), and they can be filtered by the name of the privilege in the source system (for example, ORG.ADMIN on GitHub).

Activities

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities - Account	See "Identities" on page 684.
	Identity	Collection	Same as Identities - Collection	See "Identities" on page 684.
	Identity	Identity	Same as Identities - Identity	See "Identities" on page 684.
	Group	Group	Same as Groups	

Filter	Entity Type	Category	Property	Description
Target	Asset	Asset	Same as Access Policies - Target - Asset	See "Assets" on page 688.
	Identity	Account	Same as Identities - Account	See "Identities" on page 684.
	Identity	Collection	Same as Identities - Collection	See "Identities" on page 684.
	Identity	Identity	Same as Identities - Identity	See "Identities" on page 684.
	Group	Group	Same as Groups	
Privilege		Privilege	Child Privileges	Privilege that contains a specific child privilege. For example, search the privilege Add MFA and find every admin or similar role that can add MFA devices.
			Is Role	Filter by whether the privilege represents a role on the application.
			Origin Name	The name of the privilege in the source application.
			Source App	The app on which the privilege is managed.
			Tags	Tags associated with the privilege (for example, Production or Test Environment).
			Type	Privileges are "normalized" (grouped) to a minimal set of types across all applications. Privileges can therefore be filtered by their "normalized" Type (such as Administrative), and they can be filtered specifically by the name of the privilege in the source system (for example, ORG.ADMIN on GitHub).

Filter	Entity Type	Category	Property	Description
Activity		Activity	Date	The date when the activity was performed.
			Is Virtual	Filter on whether an activity is virtual. Virtual activities are activities that are not logged in the external system but are represented as activities in the platform, such as login events.
			Success Status	Success Status
			Tags	Tags associated with the activity.

Identities

This section describes the Identities inventory table. It shows identities and accounts (human or non-human) in your organization, including the following:

- **Identities:** A unique identity (human or non-human) that owns one or more accounts. A non-human identity could be a machine identity, an automatic identity, or any other identity that doesn't belong to a human.
- **Accounts:** A unique account (human or non-human) in a single application. A non-human account might be a workload (VM, Lambda), a service account, service principal, or even a user account employed for automated tasks.

To view the Identities page:

From the left navigation, select **Inventory**, then **Identities**.

The inventory page opens to display all the identities and accounts in your organization. You can drill down into an identity or account for detailed information. For example, you can click on an identity to see what assets they can use, what privileges they have on those assets, and how they got those privileges (directly, through an IDP, or through a group membership or role).

You can toggle between these views:

- **Identities view:** List of all the unique identities.
- **Accounts view:** List of identities according to their accounts.

Multiple accounts that belong to one identity are shown differently:

- In the Identities view, they are shown as one account. By default, they are merged by matching the email address. To change the merge method, see ["Customizing Identity Merging Rules"](#) on page 696.
- In the Accounts view, they are shown as separate accounts.

When switching views, page filters remain active.

The inventory pages display information that was either gathered from integrated systems or entered manually and then processed by the platform.

Filtering and Modifying the Identities Table


By default, the Identities inventory table is sorted by number of incidents, in descending order. To customize the table view, you can:

- Filter the content displayed

The full list of filters is described in [Inventory Filter Properties](#). You can search by using an account filter parameter to see the identities that have those accounts, or search using an identity filter to see accounts with those identities.

- Save a filter as a Collection to be used in other parts of the platform
- Change the sort order
- Change the display of columns
- Use tags
- Export the data to a CSV
- See a quick view of an entity
- Zoom in on an entity by using its single-entity view

For more information about these filter and display options, see ["Inventories User Interface" on page 680](#).

You can also investigate an entity in Access Explorer, by clicking the Access Explorer link, . For more information, see ["Access Explorer" on page 709](#).

Insight into Identities Table Data

In the Incidents column, click the value to see all incidents related to an Identity. The Incidents page opens with the right-side viewing pane showing the first incident. To see the details of a different incident, click the other incident.

You can use the following columns to understand the user's access, as an alternative to looking at the Access Policy page:

- The Source Apps column shows the access that federated apps have granted to each identity or account. This column represents the applications the user has accounts in.
- The Access to Apps column shows the applications the user can access. For example, if the IdP is Okta, Okta is shown in the Source Apps column and all the apps that can be accessed through Okta are shown in the Access to app column.

Using Filter Options

In the Identities table, you can use the following filtering options:

- To focus on federated apps, use Account Source App to filter for the federated apps you are interested in.
- Use the Admin access, Shadow Admin Access, and Privileged access filters to find accounts or identities with these kinds of access.

Identity Filter Examples

- You can combine two filters to find an Okta user who is an admin in an AWS account.
- You can find all users with absolutely no admin rights by selecting the various admin filters and setting their value to **No**.

Customizing Identity Merging Rules

Identity merging is the process by which different user accounts are merged into one identity. By default, Delinea Platform merges accounts based on matching email addresses. The identity is named using the user's first and last names or, if that can not be determined, the email address. Instead of merging accounts based on matching email addresses alone, you can customize the way that user accounts are matched by setting up your own merging rules.

Merging the identities can take up to a few hours, depending on the environment size and the merging rules.

To change the default merging rules:

1. From the left navigation, choose **Settings > Identity Merging**.
2. Select one of the following options:
 - **Merge accounts with the same email**
(Default) Merges accounts that have identical email addresses.
For example, the following accounts will be merged into the same identity:
Account 1 (email): asmith@delinea.com
Account 2 (email): asmith@delinea.com
 - **Merge accounts with the same employee ID**
Merges accounts that share the same employee ID.
For example, the following accounts will be merged into the same identity:
Account 1 (employee ID): 1033394
Account 2 (employee ID): 1033394
 - **Merge accounts with the same email prefix**
Merges accounts that share the same email address prefix.
For example, the following accounts will be merged into the same identity:
Account 1 (email): asmith@delinea.com
Account 2 (email): asmith@acme.com
 - **Merge accounts with the same full name**
Merges accounts with identical first and last names.
For example, the following accounts will be merged into the same identity:
Account 1 (full name): Adam Smith
Account 2 (full name): Adam Smith

- **Merge accounts matching full name to first name initial with last name**

Merges accounts where one has a full name and the other has the first name initial followed by the last name.

For example, the following accounts will be merged into the same identity:

Account 1 (full name): Adam Smith

Account 2 (first name initial + last name): ASmith

- **Merge accounts matching email prefix to first name initial + last name**

Merges accounts where the email prefix matches the first name initial and last name.

For example, the following accounts will be merged into the same identity:

Account 1 (email): asmith@delinea.com

Account 2 (first name initial + last name): A.Smith

- **Merge accounts with the same email prefix matching to username/Login**

For example, the following accounts will be merged into the same identity:

Account 1 (email): asmith@delinea.com

Account 2 (username): asmith

- **Merge accounts with the same email matching exactly to username/Login**

For example, the following accounts will be merged into the same identity:

Account 1 (email): asmith@delinea.com

Account 2 (username): asmith@delinea.com

- **Merge accounts with the same email but replace**

Specify a replacement string to use when merging accounts with the same email address. You can define multiple such rules.

Example:

Merge accounts with email addresses that contain "_user", and replace "_user" with nothing (no replacement string specified).

Result:

The accounts adam_user@delina.com and adam@delinea.com will be merged into the same identity.

- **Merge accounts using regular expression pattern and replace**

Use regular expressions to create a more advanced merging configuration. You can define multiple such rules. Matching is case-insensitive.

Example:

Accounts starting with any number should be merged to "admin_".

Result:

419asmith@delinea.com is merged into admin_asmith@delinea.com.

Account MFA Factors

Organizations often lack comprehensive visibility into the Multi-Factor Authentication (MFA) factors used across their environment, resulting in risks that include the following:

- **Security Gaps:** Accounts without MFA or using weak methods (e.g., SMS-based) are more susceptible to compromise.
- **Compliance Risks:** Difficulty in enforcing and auditing strong authentication policies across all users.
- **User Risk Management Challenges:** Inability to easily identify high-risk user accounts that rely on weak or outdated MFA methods.

Viewing MFA Factors

To view an account's MFA factors, follow this procedure:

1. From the left navigation menu, select **Inventories**.
2. Select **Identities**.
3. On the Identities page, select **Accounts**.
4. Select an **Identity**.
5. On the panel that opens to the right, select the **MFA Factors** tab to view this information:
 - **Factor Name:** As reported by the source system (e.g., mobilePhone in Entra).
 - **Type:** Normalized format (e.g., SMS/Voice, Authenticator App).
 - **Strength:** The security level (e.g., Strong, Weak).

Recommendation: Ensure robust protection by enabling only MFA factors classified as **Strong**.

MFA Factor Types and Risks

Strong

- **Authenticator App:** Requires manual entry of a time-based code, reducing susceptibility to automated attacks.
- **FIDO2:** Enforces user presence with hardware-backed credentials.

Moderate

- **Push-Based Authentication:** Subject to push fatigue—users may approve prompts without scrutiny.

Weak

- **SMS/Voice:** Vulnerable to SIM-swapping and phishing attacks.
- **Email:** Risky if the email account is compromised.

Security Check: Disable Weak MFA Factors for All Users

To prevent unauthorized access and align with best practices for identity protection, disable weak factors for all user accounts—such as SMS/Voice or Email methods—and enable only strong MFA methods, such as Authenticator App

and FIDO2.

Groups

The Groups inventory table shows all entities that grant permissions to multiple accounts. This could be an IdP group (for example, a group of engineers using the same design tools to build their product or application) or an AWS role granting similar actors the same permissions.

The Groups page displays all the groups in your organization. You can see how many groups you have, how many incidents are opened in their name, and how they are tagged.

The Groups table displays the applications in which the groups are managed, not the applications to which those groups grant access.

You can see how many groups you have, how many incidents are opened in their name, and how they are tagged.

To view the Groups page:


From the left navigation, select **Inventory**, then **Groups**.

Filtering and Modifying Groups Table

By default, the Groups table is sorted by number of incidents, in descending order. To customize the table view, you can:

- Filter the content displayed (see "Inventory Filter Properties" on page 683)
- Save a filter as a Collection to be used in other parts of the platform
- Change the sort order
- Choose which columns to display
- Use tags
- Export the data to a CSV file
- See a quick view of an entity
- Zoom in on a group by displaying its single-entity view

For more information about these filter and display options, see "Inventories User Interface" on page 680.

You can also investigate an entity in Access Explorer by clicking , as described in "Access Explorer" on page 709.

Insight into Groups Table Data

To get further understanding of the data in the Groups table:

- In the Incidents column, click the value to see all incidents related to an Identity. The Incidents page opens with details of the first incident displayed in the right-side viewing pane. Click a different incident to see its details on the right.
- The Origin type column displays the type of object in the system it came from, providing context about what is included in the group.

Assigning Alternative Group Names

To provide additional information to users reviewing groups, you can add an alternative name to a group by using the group's inventory. Alternative names will be seen across the platform (not just by reviewers).

To add an alternative name to a group:

1. To the right of the group name, click the edit icon.
2. Enter an alternative name, then click **Save**.

Assets

The Assets inventory table shows assets such as virtual machines, applications, and repositories that are monitored by the Delinea Platform. Assets are objects monitored by the platform that you can govern, such as files and folders, databases, virtual machines, and applications.

The Assets page displays the assets in your organization in a simple table that shows the asset type (both in the platform and at the source), how many open incidents are associated with it, and the associated tags.

To view the Assets page:

From the left navigation, select **Inventory**, then **Assets**.


Filtering and Modifying Assets Table

By default, the Assets table is sorted by number of incidents, in descending order.

To customize the table view, you can:

- Filter the content displayed (see "Inventory Filter Properties" on page 683)
- Save a filter as a Collection to be used in other parts of the platform
- Change the sort order
- Choose which columns to display
- Use tags
- Export the data to a CSV file
- See a quick view of an entity
- Zoom in on an asset by displaying its single-entity view

For more information about these filter and display options, see "Inventories User Interface" on page 680.

You can also investigate an entity in Access Explorer by clicking , as described in "Access Explorer" on page 709.

Insight into Assets Table Data

To get further understanding of the data in the Assets table:

- The Type column displays the platform "normalized" type name (for example, all types of databases are referred to as "database").

- The Origin Type column displays the type names from the original product (for example, MySQL).
- In the Incidents column, click the value to see all incidents related to an Identity. The Incidents page opens with the right-side viewing pane showing the first incident. Click a different incident to see its details.

Memberships

The Memberships inventory shows all the members of all the groups on your system. The members can be user accounts, service accounts, or other groups. The inventory also shows the type of access (direct or indirect) to the group.

To view the Memberships page:


From the left navigation, select **Inventory**, then **Memberships**.

Filtering and Modifying Memberships Table

By default, the Memberships inventory table is sorted by number of incidents, in descending order. To customize the table view, you can:

- Filter the content displayed (see "Inventory Filter Properties" on page 683)
- Save a filter as a Collection to be used in other parts of the platform
- Change the sort order
- Choose which columns to display
- Use tags
- Export the data to a CSV file
- See a quick view of an entity
- Zoom in on an entity by displaying its single-entity view

For more information about these filter and display options, see "Inventories User Interface" on page 680.

You can also investigate an entity in Access Explorer, by clicking , as described in "Access Explorer" on page 709.

Using Filter Options with Memberships

You can filter the results in the Memberships table with the Actor, Target, and Access filters.

- **Actor:** Select **Identity** or **Group**, then click **+** to select an identity or group (default is all identities and groups). The filter properties are the same as those described in the Identities Filter row in "Identities" on page 684.
- **Target:** Click **+** to select a specific group. The filters are the same as those described in "Groups" on page 687.
- **Access:** To see entities with direct access to the group, select **Yes**. To see entities with indirect access, select **No**.
If you select nothing, entities with both direct and indirect access are displayed.

Access Policies

An access policy is a combination of an entity and its specific access permissions for a specific asset.

There are two main types of access policies:

- **Grouping:** group accounts or other groupings together
- **Permission:** grant A access to B with privilege Y

Examples:

- A group through which someone gains access to a resource or entity
- A direct access to a resource with certain privileges
- Assignment to a role in AWS
- Profile assigned to a user in Salesforce (SF Profile=Group)

To view the Access Policies page:

From the left navigation, select **Inventory**, then **Access Policies**.

Filtering and Modifying Access Policies Table

To customize the table view, you can:

- Filter the content displayed (see ["Inventory Filter Properties" on page 683](#))
- Save a filter as a Collection to be used in other parts of the platform
- Change the sort order
- Choose which columns to display
- Use tags
- Export the data to a CSV file
- See a quick view of an entity
- Zoom in on an entity by displaying its single-entity view

For more information about these filter and display options, see ["Inventories User Interface" on page 680](#).

Privileges

A privilege is any permission associated with access to an asset; for example, a read privilege on a file.

The Privileges page displays privileges that were either gathered from integrated systems or entered manually and then processed by the Delinea Platform.

To view the Privileges page:

From the left navigation, select **Inventory**, then **Privileges**.

Filtering and Modifying Privileges Table

By default, the Privileges inventory table is sorted by name, in ascending order.

To customize the table view, you can:

- Filter the content displayed (see "Inventory Filter Properties" on page 683)
- Change the sort order
- Choose which columns to display
- Use tags
- Zoom in on an entity by displaying its single-entity view

For more information about these filter and display options, see "Inventories User Interface" on page 680.

Using Filter Options with Privileges

You can filter the results in the Privileges table with the following fields:

- **Child Privileges:** Actions that can be performed due to having a privilege; for example, all privileges that allow users to edit groups.
- **Type:** How privileges are categorized in the platform, based on these types:
 - **Administrative:** Tells whether the privilege is considered administrative by the system of origin; for example, a full admin or an admin on the entire IAM service of the application.
 - **Data CRUD:** Any data operation, segmented by create, read, update, delete.
 - **Metadata CRUD:** Any system operation, such as creating a virtual machine, segmented by create, read, update, detect.

Privileges can have one or more types.

Activities

The Activities inventory displays the details about IAM-related activities, such as the identity of the person that performed the activity, the asset that was affected, the source, and the privilege that enabled the activity.

You can focus on activities specific to identities, assets, or groups, either by filtering by name in the Activities inventory or by viewing its related activities in the Activity Entity view.

To see a bar graph of activity over time, click the bar graph icon at the top right of the table. When you click a bar in the graph, the table shows only those activities in the timeframe represented by the bar.

You can also view the raw log of the activity as it was fetched from the system of origin. Click on the raw log icon at the end of the table row or on the side panel displayed when clicking on the row.

To view the Activities page:

From the left navigation, select **Inventory**, then **Activities**.

Filtering and Modifying Activities Table

By default, the Activities inventory table shows activity from the past week that is nonvirtual, sorted by date in descending order.

To customize the table view, you can:

- Filter the content displayed (see "Inventory Filter Properties" on page 683)
- Change the sort order
- Choose which columns to display
- Use tags
- See a quick view of an entity
- Zoom in on an asset by displaying its single-entity view

For more information about these filter and display options, see "Inventories User Interface" on page 680.

Collections

Collections are inventory queries that are saved for future reuse. You can build a collection focused on what matters most to your role and your organization, and track status over time.

Collections are not just a way to avoid writing the same queries every day. They can also be used to build custom dashboards, detection rules, and scheduled reports.

All collections on the Delinea Platform are automatically updated daily, and can also be updated on demand.

ITP-PCCE Collections vs. Computer Collections

This section describes the differences between ITP-PCCE collections and Computer Collections.

Computer Collections

Computer Collections can track only computer assets, and they are described in [Grouping with Computer Collections](#).

ITP-PCCE Collections

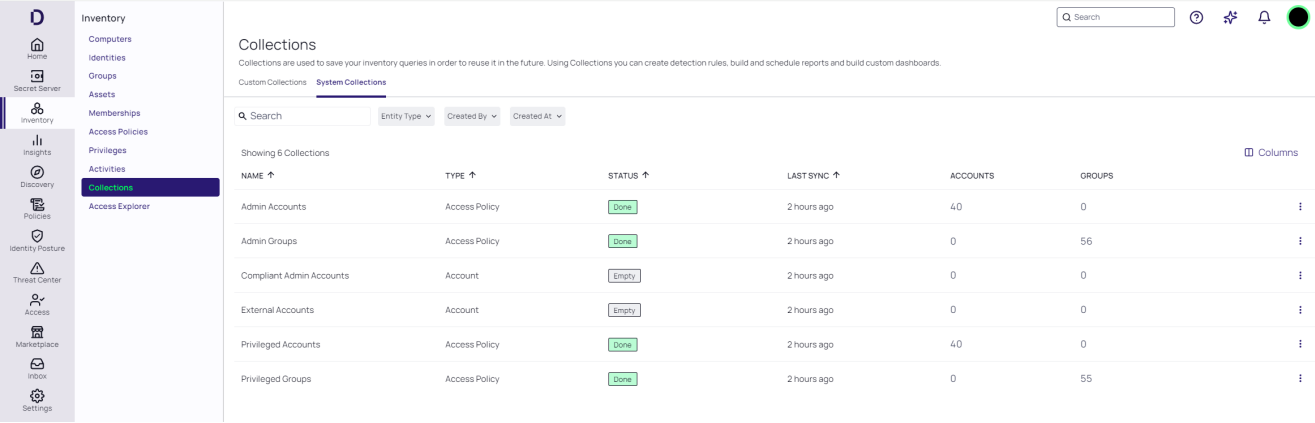
ITP-PCCE Collections can track Access Policies, Activities, Assets, Groups, Identities, Memberships, Privileges, or any combination of these. They can be either System Collections or Custom Collections. Both of these types of collections are described below.

System Collections

ITP-PCCE inventory comes with built-in System Collections, which include account and group definitions that apply system-wide, in all inventories, dashboards, and detection rules.

To view System Collections:

1. In the left navigation, select **Inventory > Collections**.
2. Choose the **System Collections** tab.

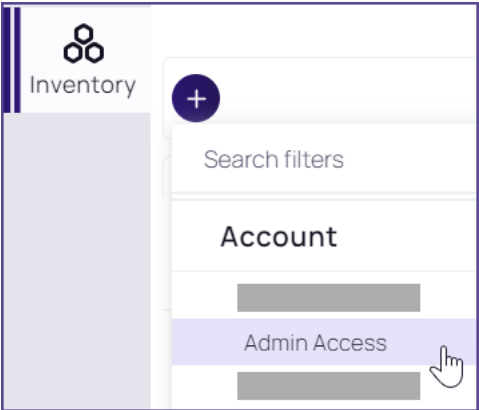


NAME	TYPE	STATUS	LAST SYNC	ACCOUNTS	GROUPS
Admin Accounts	Access Policy	Done	2 hours ago	40	0
Admin Groups	Access Policy	Done	2 hours ago	0	56
Compliant Admin Accounts	Account	Empty	2 hours ago	0	0
External Accounts	Account	Empty	2 hours ago	0	0
Privileged Accounts	Access Policy	Done	2 hours ago	40	0
Privileged Groups	Access Policy	Done	2 hours ago	0	55

The System Collections tab displays a table showing the accounts and groups, and the numbers of each, that match the System Collection definition. For each account and group, the table displays its name, type, and status information. The table also indicates whether the System Collection definitions have been modified from the default settings.

The built-in, default System Collections are as follows:

- **Admin Accounts:** Accounts with administrator privileges. Use the inventory filter **Account: Admin Access** to find Admin Accounts. For example:



- **Admin Groups:** Groups that grant Admin Account privileges to their members. Use the inventory filter **Group: Admin Access** to find Admin Groups.
- **Compliant Admin Accounts:** An Admin Account that is deemed compliant according to possession of some extra factor; for example, having an email formatted in a given format such as:
`{full_name}_adm@company.com`.
To find Compliant Admin Accounts, define a query to find all Admin Accounts with the specified email format. The Privileged Accounts dashboard displays all Compliant Admin Accounts along with the number of non-compliant accounts.
- **External Accounts:** Use the inventory filter **Account: Is External** to find External Accounts.

- **Privileged Accounts:** Accounts with privileged access.
Use the inventory filter **Account: Privileged Access** to find Privileged Accounts.
- **Privileged Groups:** Groups that grant privileged access to their members. Use the inventory filter **Groups: Privileged Access** to find Privileged Groups.

Filtering and Sorting the Collections Table

By default, the collections are sorted by date of creation, in descending order. To change the data displayed in the table, use the filter controls above the table. The selections you make are shown in the filter bar. For more information about the filter and display options, see ["Inventories User Interface" on page 680](#).

To search for a custom collection by name, type text into the search field at the top-right of the table.

Insight into Collections Table Data

To get further understanding of the data in the Collections table:

- The Type column shows which inventory the custom collection was created from.
- The Status column shows the following values:
 - Calculating
 - Exceed results: Results are too large. Run the collection query again with narrower filters to reduce its size.
 - Empty: The search yielded no results.
 - Done
 - Error
- The Results column shows how many entities matched the filters in the custom collection. To see the actual results, click the number in this column.

To see details about a collection, click the collection row in the table. A window opens to show details about the collection, including the query that created the collection, a description (if one was entered when the collection was created), and the last sync date.

The trend line detects rapid changes and shows how your collection changes over time, such as privilege creep, new admins, or shadow admins.

Configuring System Collections


From the System Collections tab, you can:

- **Edit a collection:** Edit a system collection to customize the values according to your organization's needs. See ["Editing a System Collection" on the next page](#).
- **Duplicate, then modify a collection:** Duplicate a system collection and then modify it for other needs. For example, you might want to trigger an alert for more limited matches than are defined by the system collection. See ["Duplicating and Modifying a System Collection" on the next page](#).
- **Reset a collection to default values:** Set an edited system collection back to the system default. See ["Resetting a System Collection to Default" on the next page](#).

- **Calculate collection results:** Initiate an immediate calculation of the matched accounts and groups instead of waiting for the next scheduled recalculation. See ["Calculating Collection Results"](#) below.
- **Create a new detection rule based on a collection:** Create a detection rule based on the system collection. See ["Creating a Detection Rule from a Custom Collection"](#) on the next page.

Editing a System Collection

You can edit a System Collection to customize the values according to your organization's needs.

 **Important:** Although you can edit a System Collection definition, remember that a System Collection definition impacts the entire platform, so you must proceed with caution. Consider customizing a System Collection definition only for temporary purposes, and remember to reset the System Collection back to the default values when you are finished. See ["Resetting a System Collection to Default"](#) below.


1. Hover over a system collection.
2. From its **More** menu, select **Edit**.
3. Edit the filter values.
4. Click **Save**.

In the Default column, the value changes to Edited. Results will be shown after the next result refresh. To see the results sooner, see ["Calculating Collection Results"](#) below.

Duplicating and Modifying a System Collection

You can duplicate a collection and then rename and modify the duplicate for other needs. For example, you might want to trigger an alert for more limited matches than are defined by the original collection.

1. Hover over a system collection.
2. From its **More** menu, select **Duplicate**.
3. Edit the filter values and click **Save**.

 **Note:** The System Collections tab shows only the collections that are defined by the system. Duplicated system collections are displayed in the Custom Collections tab.

Resetting a System Collection to Default

You can set an edited system collection back to the system default values.

1. Hover over a system collection where the value in the Default column is Edited.
2. From its **More** menu, select **Reset**.

The collection value returns to the default definition. In the Default column, the value returns to Default.

Calculating Collection Results

When a collection is changed, the platform automatically begins to calculate the accounts and groups that match the definition. While this is taking place, the status value changes to Calculating. You can work elsewhere while the calculation is processed, or you can calculate collection results immediately by using the following steps.

To calculate collection results immediately:

1. Hover over a system collection.
2. From its **More** menu, select **Calculate**.

The calculation is initiated immediately. Results are shown as soon as they are ready.

Custom Collections

Custom Collections are not just a way to save you from writing the same queries every day. They can help you focus on what matters most to you in your role within your organization and track status over time.

Custom Collections can also be used to build custom dashboards, scheduled reports, and new detection rules. See "Creating a Detection Rule from a Custom Collection" below.

All Custom Collections on the platform are updated automatically every day, and can also be updated on demand.

To view Custom Collections:

1. From the left navigation menu, select **Inventory > Collections**.
2. Click the **Custom Collections** tab.

NAME	TYPE	RESULTS	STATUS	CREATED BY	CREATED AT	LAST SYNC
Active Users	Account	899	Done		06/18/2024	2 hours ago
Collection 123	Computer	64	Done		07/01/2024	2 hours ago
Identity Provider	Asset	9	Done		06/18/2024	2 hours ago

Saving a Custom Collection

A custom inventory query of cloud service users can be saved for later re-use as a Custom Collection.

To save a custom collection:

1. Filter an inventory table.
2. Click **Save**.
3. In the Collection Creation dialog, enter a name.
4. (Optional) Enter a description.
5. Click **Save**.

The saved custom collection is displayed in the Collections table (select **Inventory > Collections**).



Note: Saving a custom collection may take some time.

Creating a Detection Rule from a Custom Collection

You can create a custom detection rule based on the filter criteria of a Custom Collection.

This feature is not available for custom collections created from the Computers inventory.

To create a detection rule from a custom collection:

1. From the Collection page, open the **More** menu at the far right of the desired collection, then select **Create New Detection Rule**.
2. Name the new detection rule, then click **Create**.
The Detection Rules page is displayed with the side panel open.
3. From the side panel, configure the detection rule, as described in Detection Rules.

Access Explorer

The Access Explorer provides a visual representation of the relationships between identities, assets, and access policies. It displays membership or access policies based on the filter and source selected.

You can use the Access Explorer to find out the following:

- How a cloud identity gains access to an asset
- Which cloud identities have access to an asset
- When access or membership was granted

Each rectangular block in the Explorer contains an icon that represents the cloud entity type (Asset, Identity, Account, or Group) or a logo that represents an application, as well as a name and type.

Direct vs. Indirect Access

Cloud service users can have direct or indirect access.

- **Direct access:** The actor has been assigned permission to an asset directly. For example, a cloud service user has read access to a file.
- **Indirect access:** The cloud service user has permission because they belong to a group or a role that enables access.

The following examples show how this is displayed in the Delinea Platform.

Direct Access Example

Inventory

IdentitiesGroupsAssetsMembershipsAccess PoliciesActivities

FromIdentity

+

ToAsset

+

WithAccess

Direct Access

Equals

Yes

+

Showing 10,814 Access Policies

Columns

Actor Name	Actor Type	Privilege Type	Origin Privilege	Target Name	Direct Access
<div>John Gregory</div> <div>john.gregory@acme.com</div>	User	Use	Use	<div>Okta - d...</div> <div>Applicati...</div>	Yes

Access Explorer

3D Threat Hunting & Exploration

From

AccountJohn Gregory

ToAsset

AND

Asset IDInOkta - dev-40293056

+

WithAccess

+

John Gregory

User

Has Privilege

Okta - dev-40293056

Application

When you click the Access Explorer link, the Access Explorer shows that John Gregory has direct privileges to Okta.

Indirect Access Example

Inventory

Identities Groups Assets Memberships **Access Policies** Activities

From Identity | AND Account Last Name In Gregory +

To Asset +

With Access | Direct Access Equals No +

Showing 12 Access Policies

Actor Name	Actor Type	Privilege Type	Origin Privilege	Target Name	Direct Access
John Gregory john.gregory@acme.com	User	Unknown	user.authentication.sso	Workday Applicati...	No

Access Explorer 3D Threat Hunting & Exploration

From Account | John Gregory

To Asset | AND Asset ID In Workday +

With Access +

John Gregory User — Member — O365 Group — Has Privilege — Workday Application

When you click the **Access Explorer** link, the Access Explorer shows that John Gregory is a member of the O365 service user group, and that the group has privileges to Okta.

In the Memberships and Access Privileges inventories, if you remove the Direct Access = Yes setting (because you want to show all entities, even if their access is indirect), the “Showing partial results of Memberships” message may be displayed. This indicates that calculating full *effective access* may take some time. To show the complete effective access list, create a Collection, which will calculate while you are working elsewhere.

To use the Access Explorer:

1. In the **From** field, select a source type (Identity, Account, Asset, or Group), then select the entity, such as a cloud service user or an asset.
If the Access Explorer was opened through one of the inventory views, the From source is already selected.
2. In the **Target** field, select an option. The options vary depending on what you chose in From. The filters available are the same as those in the inventory in the From selection. For details about the filters, see “Inventory Filter Properties” on page 683.
3. In the **Access** field, select an option. The options are the same as those in the Access Policies or Memberships inventory, except that “Direct” and “Limit Inheritance” are not available here. That is because the Access Explorer is limited to one source, so it can show that source’s full range of access, without any calculations. The

data in the Access Policies and Memberships inventories is for multiple sources, so the range is less and it may need time to calculate.

Minimizing the Filter Bar

To minimize the filter bar, click the up caret in the filters section.

Grouping of Similar Entities

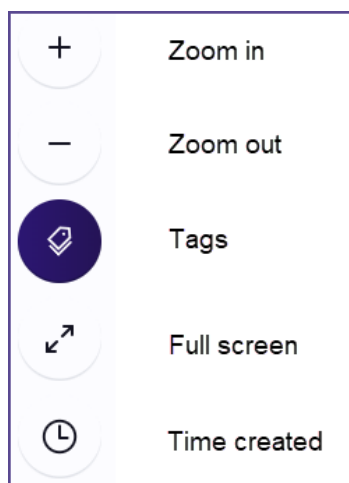
To save space in the Access Explorer graph, the platform automatically groups similar entities (assets, accounts, identities, or groups) when their privileges and applications are the same.

When looking at a group, Users and Identities are consolidated.

You can double-click on a grouping to display its contents.

Access Explorer Controls

In the bottom left corner of the Access Explorer graph is a control menu.



You can select **Time created** to see which accesses were created during a specific time. Click the clock and select a time period.

Focusing on an Object

Double-clicking an object designates the object as the Source.

- When double-clicking an identity, you are shown all the assets it can access.
- When double-clicking an asset, you are shown all the identities that have access to it.
- When double-clicking a group or role, you are shown all the assets its members can access.
- When double-clicking an account, you are shown all the assets it can access.

Moving a Node

To move a node, click and drag it while holding the mouse button.

Highlighting a Path

You can highlight a path from a node back to its source to see the full path of permission.

To highlight, click a node.

Quick “Hover” View

Quick views are available throughout the platform, providing useful information about the entity. In the Access Explorer graph, you can get information about each entity by hovering over it.



Note: Click the title in the Quick View to open its single entity page.

Recurring Reports

You can schedule reports to be generated and sent by email on a recurring basis, so you can receive the most relevant information directly in your inbox.

You can define reports based on the following:

- **Collection queries:** The results of a collection query
- **Incidents:** All changes in incidents in the last 30 days

To view the Reports page:

From the left navigation, select **Insights > General Reports**.

The Reports page shows the reports that are currently scheduled. When you hover over a report, you can delete, edit, or immediately download the report.

To create a scheduled, recurring report:

1. From the left navigation, select **Insights > General Reports**.
2. Click **Schedule a Report**.
3. Enter a name for the report.
4. Select the type of report to generate.
5. Select the frequency.
6. Enter the email addresses to receive the report.
7. Click **Create**.

Identity Posture

Enhance your visibility into the security posture of your applications and systems with a focus on preventative security measures. Reduce risk and prevent breaches with continuous monitoring of identity misconfiguration, stale access, and over-privileging.

- **"Using Apps Overview" on the next page** tells how to monitor the health of all connected cloud service user applications, both out-of-the-box and custom.

- "Using Checks" on the next page gives a structured security view for IAM/IT and security teams of how your company complies with best-practice configuration recommendations relating to identity misconfiguration, stale access, and over-privileging.

Using Apps Overview

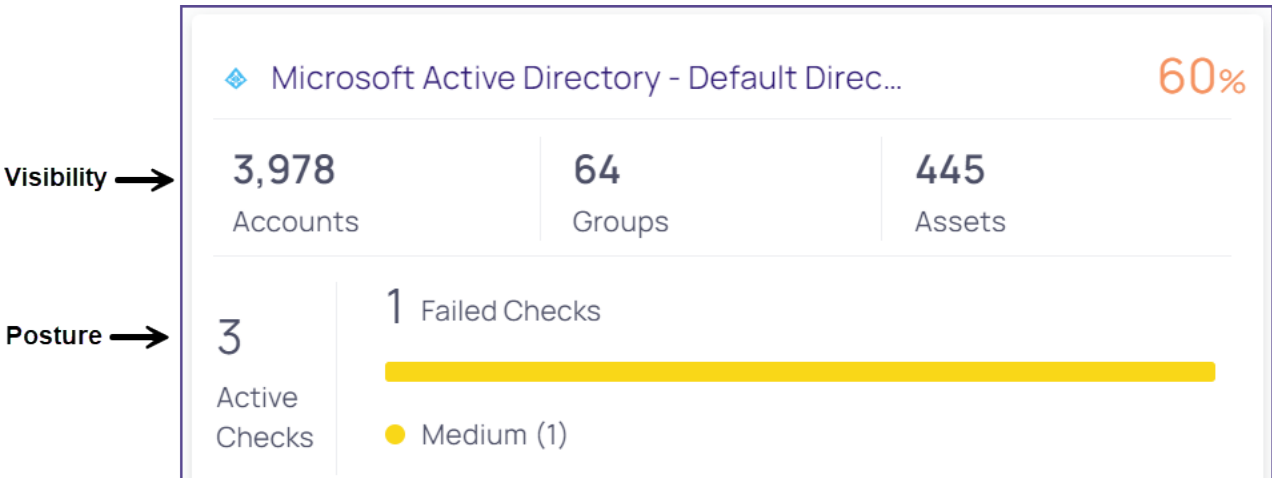
In the Apps Overview page, you can monitor the security posture of all connected cloud user applications, sorted by posture score. This page shows the health of all connected cloud user applications, both out-of-the-box and custom. The Delinea Platform assigns an identity posture score to every application to help you understand the application's state of compliance with best-practice configuration settings. For more information, see "Using Checks" on the next page.

From the Apps Overview page, you can use the identity posture score to easily find those applications that are most vulnerable, then drill down to see exactly which issues you need to manage.

To display the Apps Overview page:

In the left navigation, select **Identity Posture > Apps Overview**.

Every application is represented by a tile.



The app tiles are sorted in ascending order by posture score, from 0% (greatest risk) to 100% (least risk). The app with the lowest posture score, which represents the greatest risk, is displayed first. You can filter the page to show one type of app at a time.

The information for each app is presented in two sections:

- **Visibility:** The number of accounts, groups, and assets.
- **Posture:** The number of checks performed and failed, and the severity of each failed check. For more information, see "Using Checks" on the next page.

Click any field to see the supporting data in the platform. For example, when you click the app title, the Checks page displays, filtered by that application. You can easily drill down for further explanation of the app status.

To focus on relevant apps, you can filter the page by application type, or type search terms into the search field.

Using Checks

The Checks page gives a structured security view for IAM/IT and security teams of how your company complies with best-practice configuration recommendations (“checks”) relating to identity misconfiguration, stale access, and over-privileging. This page shows a catalog of security checks that provide visibility into the preventative security posture of your applications and systems.

For example, the Enable MFA (Multi-factor Authentication) for All Users check shows the level of MFA enrollment within the organization.

Onboarding Process

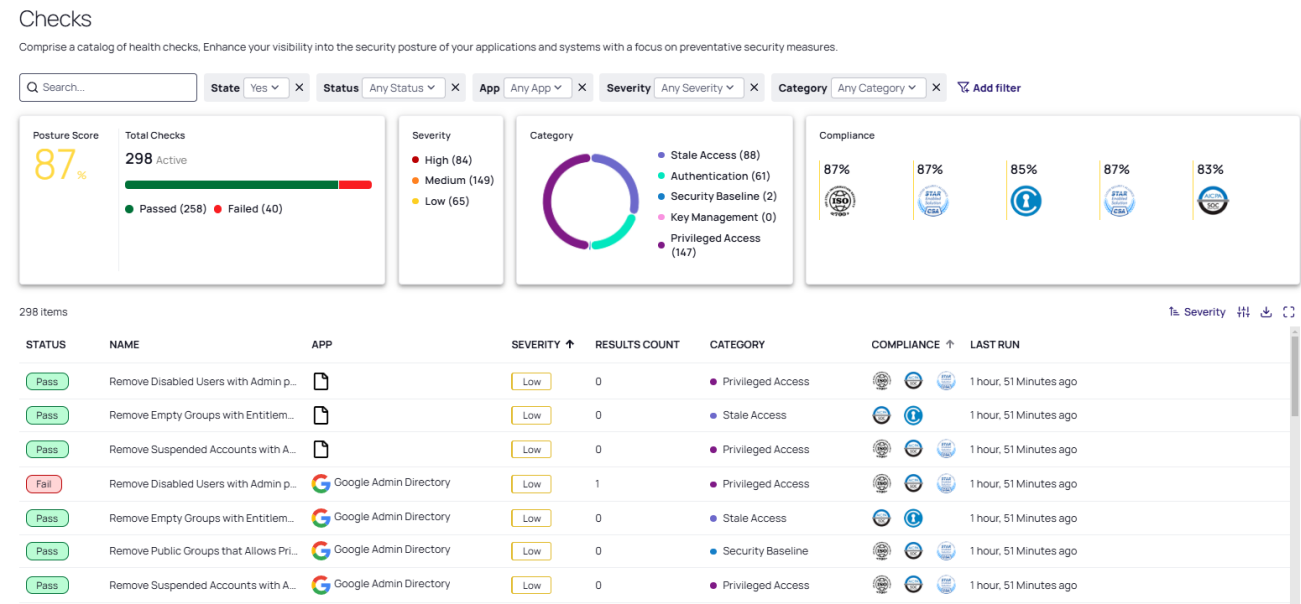
The onboarding process does not require additional permissions. Start by updating check severities if necessary and disabling irrelevant checks.

To effectively engage with the Identity Posture functions, begin by exploring the **Apps Overview** page to identify the most vulnerable applications. Proceed to the posture page filtered by the specific application, review all failed checks, and address them individually based on their severities, categories or compliance frameworks. See "Using Apps Overview" on the previous page.

Viewing the Checks Page

From the left navigation, select **Identity Posture > Checks**.

On the Checks page, each row represents a different check that Delinea Platform runs. These checks are based on instances of applications that are integrated with the platform.



By default, the page is sorted in descending order by check severity. You can change the sort order by clicking a column heading.

The checks are divided into categories to streamline management:

- **Authentication:** Mechanisms used to verify the identity of cloud service users, systems, or processes
- **Privileged access:** Management of access rights for cloud service users with elevated permissions
- **Stale access:** Management of outdated or unused access rights
- **Security baseline:** Base configurations of the application
- **Key management:** Management of keys

The table displays basic information and the compliance frameworks relevant to each check. The **Results Count** column displays the number of entities (*Affected Entities*) that failed the check.

Best Practices for Checks

For best results, follow these recommendations.

- Have a posture score of at least 90% for each application.
- Solve all high severity checks within a week, medium severity checks within two weeks, and low severity checks within a month.
- Regularly monitor the posture pages and posture scores for your connected applications to identify configuration drifts and degraded checks. Review once a week to detect any misconfigurations in a timely manner.
- Engage your app owners in reviewing and addressing any misconfigurations.

Diagnosing Issues with the Checks Side Panel

On the Checks page, click any row in the table. The Checks side panel opens, displaying more information about the check.

General Tab

On the **General** tab, the **Description** includes the function of the check and the security motivation for remediating the Affected Entities.

Disable a Check

To disable a check, click **Disable**.



Note: Disabling a check decreases your overall identity posture score. Click **Disable** only if your organization is unable to follow the best-practice recommendations, and is willing to accept the risk of a misconfiguration.

Change a Check's Severity

To change the severity of a check, select a different setting from the **Severity** drop-down menu.

Remove Empty Groups with Entitlements

Disable

Show details

General

Affected Entities

Remediation Steps

^

Description

Tracks empty groups that still have access policies, meaning any member that joins those groups will be able to gain those privileges.

Empty groups with entitlements can lead to undesired access to assets the group is entitled to.

^

Properties

App Name

Microsoft Entra ID - Authomize

Status

Fail

State

Enabled

Severity

Low

Affected Entities

2

Category

Stale Access


Compliance


Last Run

1/9/25, 11:31 AM


Affected Entities Tab

The **Affected Entities** tab displays each affected entity. Click any entity to expand its panel, where you can view the detailed **Description** and the remediation **Recommendation**.

 **Enable MFA for all Admins**



Disable




Show details

General


Affected Entities


Remediation Steps

 Search...

State



Included









2 items

Card view

  John Doe



  Jane Doe



Status

Included


Description

Ping Identity admin user John Doe has no multi factor authentication (MFA) set up.

Recommendation

Ensure that John Doe enables MFA.

Vault an Affected Entity or Exclude it from a Check

 **Note:** Excluding an Affected Entity from a check can change the status of the check; for example, if all entities are excluded, the check will always pass.

To exclude a specific Affected Entity from a check:

1. Click the entity to expand its panel.
2. On the desired entity, hover your cursor to the left of the up caret, click the three dots, then select **More actions**.

Unvaulted PAM Bypassing using Credentials

Show Full Page

General Affected Entities Remediation Steps

Search... State Included X

Review results in inventory

6 items Card view

SNOWFLAKE

ROI

More actions

3. Select **Exclude** from the drop-down menu. Excluded entities are moved to the Excluded list.


Exclude

Vault account credentials



To vault an unvaulted Affected Entity, select **Vault account credentials**.

Remediation Steps Tab

The **Remediation Steps** tab lists the steps recommended to remediate a failed check.



Enforce Password Policy


Disable


[Show details](#)

General
Affected Entities
Remediation Steps

^ Suggested Steps

Security > Authenticators > Passwords

Ensure all Password policies require the following:

- Lower case letter
- Upper case Letter
- Numbers
- Symbol
- Does not contain part of username
- Does not contain part of first name
- Does not contain part of last name
- Restrict use of common passwords
- Enforce password history for last 4 passwords.

Admin and Privileged Access

This topic distinguishes Admin Access from Privileged Access on the platform.

To more effectively control user access, you can create customized definitions for *Admin Access* and *Privileged Access* under [System Collections](#).

Admin Access

Admin Access applies to any account with full control over the system or the IAM model of the application.

Here's how it works:

- For each integration type (such as *cloud provider* or *identity platform*) specific permissions are identified as administrative.
- We then search for any **roles** that include these admin-level permissions.
- Specifically, we look for entities with admin-type permissions to access to top-level resources such as:

- Application
- Project
- Subscription
- Service
- Domain

These definitions are part of the *admin access system collection*. All admin-related access controls are based on this logic, and customers can customize this collection to match their internal policies.

Privileged Access

Privileged access is more flexible than admin access, and it can vary by organization. Generally, it refers to users who have powerful, potentially risky permissions, such as:

- Deleting a database or virtual machine (VM)
- Adding new applications to identity providers
- Disabling Windows services

This is also defined in a system collection. We provide a broad default definition, but we strongly recommend that customers review and refine it to meet their specific security needs.

Shadow Admins

The Delinea Platform Shadow Admin engine discovers Shadow Admin cloud service users in IaaS providers who can perform privilege escalation but can't manage the whole IAM model. This discovery can be performed by configuring authentication and authorization resources and by assigning roles to others.

An AWS shadow admin is a cloud service user (cloud identity) who can perform one or more of the actions listed in the following table, in one of the policies attached to it.

AWS Actions

Action	Enables a cloud service user to...
CreateAccessKey	Create an access key for another IAM user.
CreateLoginProfile	Create a password for an IAM user.
UpdateLoginProfile	Reset their user password.
AttachUserPolicy / AttachGroupPolicy / AttachRolePolicy	Attach a different existing policy to an identity, which provides an easy way to escalate privileges.
PutUserPolicy / PutGroupPolicy / PutRolePolicy	Add or update the inline policy attached to the corresponding identity.

Action	Enables a cloud service user to...
CreatePolicy	Create new policies including an inline policy attached directly to an identity.
AddUserToGroup	Add a user to existing groups, which grants the user all privileges for the group.
UpdateAssumeRolePolicy	Chain roles, allowing a non-privileged role to assume a privileged one.
CreatePolicyVersion and SetDefaultPolicyVersion	Update policy versions to escalate privileges.
PassRole and (CreateInstanceProfile / AddRoleToInstanceProfile)	An instance profile is a role that can be attached to an EC2 instance to allow the code on it to call other services. Creating an instance profile and assigning it to instances can be used to escalate privileges.
iam:PassRole and lambda:CreateFunction and lambda:InvokeFunction	This combination of privileges allows a user to assign a role to a newly created Lambda function and invoke it. This technique can be used to hide escalated privileges and exfiltrate information.
iam:PassRole and lambda:CreateFunction and lambda:CreateEventSourceMapping	The event source is the origin of event data. This combination of roles allows an identity to sniff incoming data.
iam:PassRole and glue:CreateDevEndpoint	Creating new development endpoints in glue and assigning a role to them provides a new environment with all privileges granted by this role.
iam:PassRole and cloudformation:CreateStack	Cloud formation allows users to create AWS assets even if the user doesn't have full privileges to create all other resources.
iam:PassRole and datapipeline:CreatePipeline and datapipeline:PutPipelineDefinition	By creating new pipelines or updating roles assigned to existing ones, the attacker can control or "spy" on your organization's data in different data sources.
SetDefaultPolicyVersion	The policy version defines the AWS internal version language that the policy supports. By downgrading the version, a user can ignore fields and gain privileges that were bound to specific variables.
lambda:UpdateFunctionCode	Functions can call other AWS resources based on different trust policies in the cloud service account. By updating the code of a function, a user can escalate privileges and exfiltrate information.
glue:UpdateDevEndpoint	Glue endpoints define the environment the code will run on. Changing the glue endpoint can push code to protected environments or break your infrastructure logic.

Azure Permissions

Azure Permission(s)	Description
Microsoft.Authorization/elevateAccess/action	A cloud service user/attacker can elevate their privileges to become admins.
Microsoft.Authorization/roleDefinitions/write	An attacker can update roles and escalate to administrative privileges.
Microsoft.Authorization/roleAssignments/write	The user can assign other users to roles. A user entitled to this role can make other admins.
microsoft.directory/users/password/update	The user can reset another user's password, which can help them gain control over accounts.
microsoft.directory/users/authenticationMethods/delete	An attacker can remove a user authentication method like MFA, helping an attacker to steal an account.
Microsoft.Authorization/*/Write	The user can assign any role to an application and elevate its privileges.
microsoft.directory/servicePrincipals/policies/update	The user can update the role assigned to a service principle, which can lead to escalated privileges.
microsoft.directory/servicePrincipals/permissions/update	
microsoft.directory/servicePrincipals/enable	The user can re-enable a disabled service principle, so an attacker can find a disabled service principal with the right privileges and enable it.
microsoft.directory/groups/members/update	The user can update group members, which allows the user to escalate privileges by adding the account to more privileged groups.
Microsoft.ManagedIdentity/userAssignedIdentities/write	Managed identities are like access keys. They limit the need to manage credentials and allow applications to access resources.
microsoft.directory/users/create	The user can create new local users in active directory/Azure.
microsoft.directory/users/password/update	
Microsoft.Authorization/classicAdministrators/write	The user can add other users as administrators.

Threat Center

In Threat Center, you can manage alerts and alert collections called cases to swiftly identify threatening actions and respond promptly to mitigate each issue.

- [Cases](#): A case is an aggregated set of alerts that together represent a meaningful security finding.
- [Viewing Alerts](#): Select **Threat Center > Alerts**.
- [Alerts Details](#): Click the **Alert Name** to view its details panel.
- [Resolving Alerts](#): Each new alert is unresolved by default.



Note: Throughout this chapter on ITP/PCCE, the terms **users**, **accounts**, and **identities** generally refer to cloud service users/accounts or cloud identities, and not to Delinea Platform users.

Using Cases

A **case** is an aggregated set of alerts that together represent a meaningful security finding.

Cases are designed to improve fidelity and reduce noise by continuously grouping alerts together. For example, if an actor is being targeted by a brute force attack, this might generate multiple findings over a period of time, but from a case perspective you will see only a single case about this entity. This single case represents the aggregation of all relevant findings about this user so you don't need to skim through a list of non-related findings, but can single out the item that your SOC team needs to take care of.

Case Management

A case rule is a set of security conditions. When the conditions are met, the rule triggers a case for the security team to examine. For example, the brute force case rule generates a case or appends items to an existing case based on the rule logic, every time a new alert about a single brute force attempt is found.

The rule engine runs autonomously, checking data whenever a new integration is enabled, when new activities appear in the system, and periodically thereafter.

To view the case management page, select **Threat Center > Case management**.

The Detection Rules Table

Column	Description	Example values
Title	The title of the case rule	Account under brute force attack
Severity	Severity of the detection rule	Critical, High, Medium, or Low
Status	The case rule status	Enabled: Case are created. Disabled: Case rule is not active, and new case are not created.
MITRE	Related MITRE ATT&CK tactics	For example: Credential access, Initial access, Defense evasion

Column	Description	Example values
Apps	The applications that the detection rule tracks	AWS, Okta, GCP, GitHub and more
Categories (hidden until selected)	The categories to which the detection rule belongs	Threats, Privileged Access, Stale Access, Key Management, Security Baseline, Authentication
Compliance (hidden until selected)	Compliance frameworks that are relevant to the detection rule	List of relevant compliance frameworks

Filtering, Searching, and Sorting Detection Rules

To change which rules are displayed in the table, you can filter and sort its displayed data using the filters above the table. When you filter, the selections you make are shown in the filter bar. To search for a case rule by name, type text into the search field.

By default, the table is sorted by the Title column in alphabetical order. To sort the table differently, click a column heading. If needed, click it again to reverse the sort order.

Case Rule Side Panel:

The Case Rule side panel provides detailed information about specific security incidents and automated response options. This documentation outlines the key components of the side panel and their functions.

General Tab

The General tab displays high-level details of the security case rule, including:

Case Definition Properties

- **Status:** Indicates whether the rule is enabled or disabled.
 - Status of a rule can be switched from enabled to disabled and vice versa by using the toggle near the status
- **Severity:** Defines the criticality of the case (e.g., High, Medium, Low).
 - Each rule has a default severity value, but this can be changed by simply selecting a different value from the severity drop-down
- **MITRE Mapping:** Specifies the associated MITRE ATT&CK category (e.g., Credential Access).
- **Category:** Defines the type of incident (e.g., Threats).
- **Compliance:** (Not provided in the screenshot but may be used for regulatory alignment.)
- **Supported Apps:** Displays the applications impacted by or supporting this case rule (e.g., Ping Identity, Okta, Azure AD).

Remediation Steps Tab

The Remediation Steps tab provides automated response actions that can be executed to mitigate the detected threat.

Automated Response Options

The available automated response workflows are grouped by application integrations such as Okta or Microsoft, an instance of a configuration will appear per each integrated source that is supported by the rule.

Each integration offers multiple response actions:

- **Disable user account** - Disables the affected user account.
- **Enable user account** - Re-enables a previously disabled user account.
- **Revoke user active sign-in sessions** - Forces the user to re-authenticate by logging them out of all active sessions.
- **Add user to group** - Adds the affected user to a specified group, when enabling this option you will be prompted to select the group to which a user will be added.
- **Remove user from group** - Removes the affected user from a specified group, when enabling this option you will be prompted to select the group from which a user will be removed.



Note: If permissions are not correctly configured for the integration, an error message appears: "You don't have permissions to activate this Automated Response. Update the Permission of the Integration."

Account under a brute force attack



General

Remediation Steps

^ Automated Response



Okta - dev-52038398-admin

5 workflows available



You don't have permissions to activate this Automated Response. Update the Permission of the Integration.



Disable user account

Disable the user account



Enable user account

Enable the user account



Revoke user active sign in sessions

Revoke the user's active sign in sessions, forcing them to log in again



Add user to group

Add a user account to a group.



Remove user from group

Remove a user from a group.

How to Review Cases

The Case Result is an interface within the security platform that presents detailed information about detected security cases. It provides insights into the nature of the attack, affected entities, timeline of events, and recommended actions.

Cases are generated by the case rule found on the case management page.

To view the case management page, select **Threat Center > Cases**.

The Cases table

Column	Description	Example values
Case	The title of the case	Account under MFA bombing attack
Alert	Number of alert this case consist of	2 - means two different alerts were aggregated to this case
Severity	Severity of this case	Critical, High, Medium, or Low
Apps	The applications of the entities found by this case	AWS, Okta, GCP, GitHub and more
Created at	Timestamp indicating when the case was first generated.	
Updated at	Timestamp indicating when the case was last updated.	
Status	The status of this case	Open - active, investigation is in progress, new alerts might be attached. Closed - investigation is done, this case is no longer active, no alerts will be attached.
Compliance (hidden until selected)	Compliance frameworks that are relevant to the detection rule	List of relevant compliance frameworks

Filtering, Searching, and Sorting

To change which cases are displayed in the table, you can filter and sort its displayed data using the filters above the table. When you filter, the selections you make are shown in the filter bar. To search for a case rule by name, type text into the search field.

By default, the table is sorted by the Created At column in descending order. To sort the table differently, click a column heading. If needed, click it again to reverse the sort order.

Case Side Panel

Case Summary

The top section of the side panel includes the following details:

- **Case Title:** A descriptive name for the security event (e.g., "Brute Force Attempt on John Doe").
- **Close Case Button:** Enables users to mark the case as resolved, once a case become closed no new alerts will be added to the same case even if they are related, a new finding will open a new case.
- **Navigation Tabs:**

- **General:** Overview of the attack, description, and recommendations.
- **Entities:** Lists affected users, assets, or any other entity.
- **Timeline:** Displays chronological logs of attack attempts.

General Tab

The General tab provides a high-level summary of the attack.

Description - What happened

Recommendations - What we recommend to do in order to expand investigation or resolve the issue

Case Properties:

- **Status:** Indicates whether the case is Open or Closed.
- **Severity:** Defined as Low, Medium, or High based on the threat impact.
- **Assignee:** Displays the name of the security analyst assigned to the case.
- **Source Apps:** Indicates the security tools or platforms detecting the event.
- **Case ID:** A unique identifier for tracking the security case.
- **Compliance:** Shows if the case relates to any regulatory requirements.
- **Created At:** Timestamp indicating when the case was first generated.
- **Last Updated:** Timestamp indicating the most recent update to the case.

Entities Tab

The Entities tab identifies the affected user, account, or system component.

Similar to alerts, the case entities can be either affected or actors

- **Affect** - represent the entities that were affected by this finding, for example in a brute force case this will be the targeted user
- **Actors** - represents the entities that initiated or took part in the case and caused the issue, for example in a brute force case those will be the IP addresses from which the user were targeted.

Timeline Tab

The Timeline tab provides a chronological sequence of security alerts related to the attack.

Example Timeline Entries

- 24/01/2025, 01:45 - Initial detection of a stealthy brute force attempt spanning multiple days.
- 25/01/2025, 03:15 - Additional failed login attempts detected.
- 25/01/2025, 03:20 - Continued unauthorized access attempts.
- 25/01/2025, 04:05 - New alert generated for another stealthy brute force attack.
- 25/01/2025, 19:40 - Latest detection of brute force activity.

Viewing Alerts

Alerts are available as part of the Threat Center.

From the left navigation, select **Threat Center > Alerts**.

The Alerts page is displayed. The Alerts table shows all the alerts that your account has permissions to view. By default, the table displays all alerts that were created in the last 30 days that have not been marked as resolved.

Q Search

?

⚙

🔔

k

Alerts

Q Search...

Apps In Any Apps X

Category In Any Category X

Created at Last 30 days X

Resolution In Unresolved X

Severity In Any Severity X

Add filter

1,662 items

Alert Name

⌵

⌵

⌵

⌵

⌵

⌵

⌵

⌵


Alert Name	Affected Entity	Affected Entity Type	Source Apps	Mitre	Compliance	Created Date	Last Detected At	Resolution
Admin account detected	Ron L	User		Initial Access +5 >	+2 >	12/3/24, 3:01 AM	1 hour, 40 Minutes ago	Unresolved
Admin account detected	David B	User		Initial Access +5 >	+2 >	12/3/24, 3:01 AM	1 hour, 40 Minutes ago	Unresolved
Admin account detected	BACKUPADMIN	User		Initial Access +5 >	+2 >	12/3/24, 3:01 AM	1 hour, 40 Minutes ago	Unresolved
Admin account detected	JOHN	User		Initial Access +5 >	+2 >	12/3/24, 3:01 AM	1 hour, 40 Minutes ago	Unresolved
Admin account detected	Ron L	User		Initial Access +5 >	+2 >	12/3/24, 3:01 AM	1 hour, 39 Minutes ago	Unresolved
Admin account detected	Ariel Z	User		Initial Access +5 >	+2 >	12/3/24, 3:01 AM	1 hour, 40 Minutes ago	Unresolved

Customizing the Display

You can control which columns are presented in the Alerts table using the Displayed Columns icon (⌵).

Use the Search box to locate a specific alert by name.

Use the cards at the top of the table to filter the data displayed in the table. Each card provides a dropdown list of parameters defined for that column. Select values in each dropdown to restrict the type of data displayed for that column. For more information, see "Filtering in List Pages" on page 48.

 **Note:** To find only the alerts related to analytics, filter the table to only show **Apps** in the **Delinea Platform**.


The following table describes the columns in the Alerts table.

Column	Description
Alert Name	A descriptive title for the alert.
Affected entity	The entity that was affected by this alert
Affected entity type	The type of entity related to the alert
Source apps	The application this alert relates to, usually the same app as of the affected entity

MITRE	The MITRE tactics the alert relates to
Category	The category of the alert as assigned by Delinea
Compliance	Any associated compliance standards. Supported standards include: SOC 2, ISO 27001, CSA 4, CSA 3, and CIS V8.
Created date	The time when this alert was created
Last Detected At	The time elapsed since the last alert was detected
Severity	The severity assigned to this detection: low, medium, or high
Resolution	Status of the alert: resolved or unresolved

Viewing Alert Details

Click the **Alert Name** to view its details panel.

 **Note:** Details may differ due to updates.

Abnormal spike in users activity

Mark as False Positive

X

General

Entities

Evidence

^ Description

An abnormal increase in activity was observed for the user shir.hirshman@authomize on 2024-12-12, with 138 actions recorded compared to their monthly average of 4.1 actions. This significant deviation from typical behavior, based on the last 30 days of activity data, may indicate potential misuse or unauthorized access and warrants further investigation to determine whether the activity is legitimate or suspicious.

^ Recommendation

Verify the actions performed by the user shir.hirshman@authomize during this time period (attached as evidence), and review security logs for any unusual activity around the time of the action taken. Consider implementing temporary restrictions on the user's action until the situation is fully assessed and clarified.

^ Alert Properties


Resolution

Unresolved

Severity

High

Affected Entity

 Shir Hirshman (Account)

Actor

-


Last Detected At

13/12/2024, 02:00

Created At

12/12/2024, 23:00

Source Apps



Mitre

-

Category

Behavior Analysis

Alert Properties

Alert Property	Description
Resolution	Status of the alert: resolved or unresolved
Affected entity	The entity that was affected by this alert
Actor	The entity/IP that performed the action in the alert
Created at	The time when this alert was created
Updated at	The last time the system scanned the issue
Compliance	The compliance standards
MITRE	The MITRE tactics the alert relates to
Source app	The application this alert relates to, usually the same app as of the affected entity
Severity	The severity assigned to this detection: low, medium, or high
Category	The category of the alert as assigned by Delinea

In addition to the basic descriptions of alert properties, additional controls are available using the tabs in the Alerts page.

General Tab

Provides details about what was detected, as well as general alert properties. For a description of the columns in this tab, see [Inventory Filter Properties](#).

Entities Tab

Displays the entities that are affected or related to the alert or the actor who caused the issue. Alerts can be connected to the following types of entities:

- Affected: Who was affected by the detection
- Actor: The person or IP who performed the action detected in the alert
- Related: Anything or anyone that was related to the alert but not affected directly

Evidence Tab

Displays static information that can help you understand what happened and what data the Delinea Platform had at the moment the alert was detected; for example, user IP information, session details, or a map showing the user baseline locations with the detected suspicious location. The different types of evidence give details about the alert and the information used to detect it.

Evidence for alerts can include the following types of contexts:

- **Related activities:** Timeline of the actions/activities that were taken and found to be either the root cause of the alert or related to the alert. Each line represent an action taken by a user in the system.

^ **Activities** | 21 Activities

17/12/2024, 23:53:59.869

MFA Authentication | IP: 401451161 Fail

Actor: [redacted]@delinea.com Target Platform

17/12/2024, 23:53:21.229

Authentication Finished | IP: 10027423126 Fail

Actor: [redacted]@delinea.com Target Platform

17/12/2024, 23:27:39.307

MFA Authentication | IP: 401451161 Fail

Actor: [redacted]@delinea.com Target Platform

17/12/2024, 23:23:51.792

Logout | IP: 10027423126 Success

Actor: [redacted]@delinea.com Target Platform

17/12/2024, 23:21:45.011

Credential Verification | IP: 401451161 Success

Actor: [redacted]@delinea.com Target Platform

- **IPs:** Aggregated list of IPs that were included in the alert. For each IP, extra information is displayed, such as the location.

Data shown reflects a snapshot at alert creation. Current entity details may differ due to updates. Last updated: Dec 17, 2024

^ **IP's** | 1 IP

1 item

Grid view 1 Not sorted [icon] [icon] [icon]

ADDRESS	COUNTRY	REGION	IS VPN	IS PROXY	IS TOR
30104-237126	US	US-DC			

^ **Session Information** | 1 Sessions

1 item

Grid view 1 Not sorted [icon] [icon] [icon]

SESSION IDS	STARTED AT	ENDED AT	IP	USER AGENT
	17/12/2024, 18:09	17/12/2024, 19:35	30104-237126	Mozilla/5.0 (Macint...

- **Sessions:** List of sessions related to the alert. The list can be a single session or multiple sessions. Each has a start and end time and represents the timeframe when the user was active in the system. Each session can come from a different IP and user-agent. This data will be shown in this context.

- **Map:** User locations. The map can show common locations and suspicious locations. Common locations are marked in green, and suspicious locations are marked in orange.

^ Map

The map shows common user session location and the suspicious location flagged by this alert the map should show all the locations from which users perform actions, marking as suspicious the one flagged by this alert

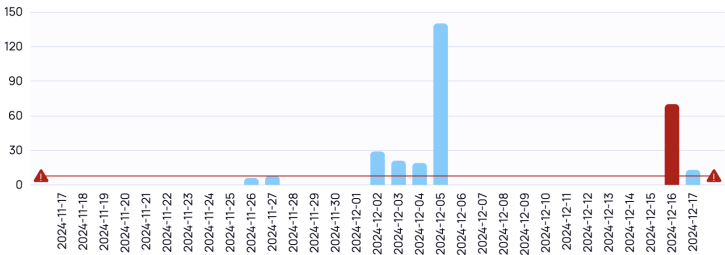


- **Burst of activities:** Bar chart showing user activities over time. For example, this can show a historical baseline of the user's administrative activities over a period of a month and highlight (in red) the anomalous day.

^ Activity counts

Activity counts per day with the abnormal activity amount highlighted

▲ average - 8



- **Heatmap:** Chart that usually shows users sessions over a period of 30 days. This chart is used to show when the user is active, the session duration, and if available, lower and upper thresholds for the user activity time.
- **Suspicious activities breakdown:** Chart that is part of the Abnormal spike in users activity alert. Shows all activities, grouped by type, that were performed by the user on the day the Delinea Platform detected a spike in activity.

Resolving Alerts

Each new alert is unresolved by default. An alert is marked as resolved and moved to a resolved state if:

- The issue can no longer be detected by the rule.
- The detection is based on activities, and 30 days have passed since the original detection. Alerts automatically resolve after 30 days.
- After reviewing the alert, you determine it is not of concern, and click **Mark as False Positive**.

Protect AI & LLMs within Cloud Apps

Through its ITP and PCCE capabilities, the Delinea Platform detects and rates the risks levels of deployed LLMs and AI agents throughout your cloud infrastructure.

Visibility into AI Models Deployed in CSPs

The Delinea Platform gives visibility into all active AI models, including their usage, ownership, and deployments—enabling alignment with organizational compliance and legal requirements.

Delinea incorporates publicly available model reputation indicators, including:

- Hallucination rates
- Fairness or privacy ratings
- Safety thresholds

This additional context supports better decision making and risk analysis in case the LLM has access to sensitive assets.

Visibility into AI agents and services managed in CSPs

AI agents are applications or services that leverage AI models (LLMs) to perform tasks, respond to user queries, or automate operations. These agents are often deployed and managed within the cloud itself or run independently on cloud assets like VMs or containers.

The Delinea Platform provides deep discovery and visibility into AI agents and services hosted and managed in Azure, including rich metadata such as:

- Underlying model and publisher
- Creation date and region
- Agent instructions and descriptions
- Associated tools (e.g., Azure Functions, API calls, files)

The Delinea Platform analyzes potential access from AI agents and alerts those with access to sensitive assets.

Visibility into AI Models Hosted on Cloud Assets

The Delinea Platform extends visibility beyond managed services to detect self-hosted or "under-the-radar" AI models, such as LLMs deployed on Azure VMs, containers, or Kubernetes clusters (AKS). This helps organizations discover AI deployments that may bypass centralized governance and identify assets that can potentially run AI without your organization's awareness.

Access Control and Risk Mapping

The Platform analyzes AI agents' configuration, including their tools, functions, and instruction sets, to:

- Identify potential access to sensitive or production assets
- Flag agents with access beyond their intended scope
- Support governance and least privilege enforcement

AI Reports for Governance

1. Navigate to **Insights > Reporting**
2. Enter AI agents to generate a report listing all known AI agents across your Azure environment.

This centralized view supports audit, compliance, and policy review.

Security Checks and Risk Assessments

The Delinea Platform runs automated risk assessments on AI & LLMs to improve IAM hygiene, including:

- LLMs operating with high temperature (risk of unpredictable output)
- AI agents lacking audit logs
- AI services exposed to the public internet
- Agents created by external accounts

Configuring Risk

By understanding risk, you can highlight the identified weaknesses and prioritize actions according to the potential impact of a security breach.

Risk configuration can be used for the following purposes:

- Prioritize the result of incidents by focusing first on the higher risk incidents
- Find the highest risk cloud service accounts or cloud identities and reduce the organizational risk

The Delinea Platform assesses account access scope, ongoing attacks, and inherent vulnerabilities in each account's security to provide a comprehensive understanding of risk.

Risk Types

The platform presents scores for the following types of cloud service user risk:

- **Overall risk:** Total risk score, combining the blast radius and takeover risk.
- **Blast radius risk:** The risk of potential damage based on how much access each cloud service account or cloud identity has. Blast radius risk incorporates account administrative access, shadow admin privileges, privileged access, and non-privileged access.
- **Account takeover risk:** The risk of a cloud service account being taken over. Account takeover risk is calculated based on relevant platform detection rules (from the detection, account takeover, and stale access categories). Risk reflects the weakness of the account (for example, lacking MFA) or if an actual attack was detected on the accounts (for example, a brute force attack).

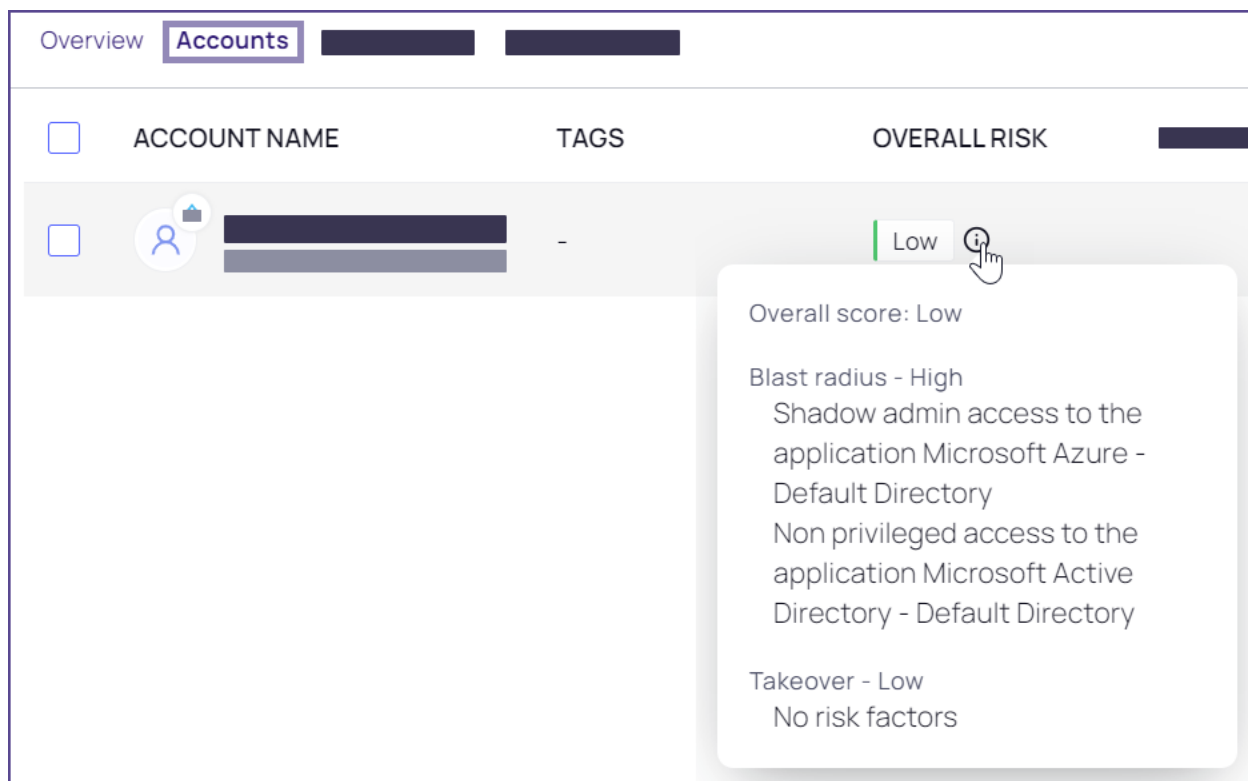
To view risk scores:

From the left navigation, select **Inventory**, then **Identities**.

You can see risk scores for each cloud service user on the **Identities** inventory tab. You might need to enable the display of these columns. For more information about this tab, see "[Identities](#)" on page 694

When you click a cloud service user, the user's risk scores are displayed on the single entity page, on both the Overview tab (summarized) and the Accounts tab (detailed).

On the Accounts tab, when you hover over the overall risk, you can see why the risk score was assigned.



Configuring Risk

Risk scores are determined by underlying risk factors. You can customize the importance and relevance (weight) of these risk factors so that the risk scores presented reflect your specific needs.

Blast radius risk is determined by the importance assigned to each access factor.


Account takeover risk is determined by the findings of each detection rule and the importance assigned to each rule. The detection rules shown are those in the Detection, Account takeover, and Stale access groups.

To configure risk:

1. In the left navigation, select **Settings > Risk Configuration**.
2. The Blast Radius tab shows the risk factors that make up the blast radius score. To see the definition of a risk factor, click its tool tip. To set levels for account takeover risk, select the **Account Takeover** tab.
3. Click an importance level for a factor. To ignore the risk factor entirely, toggle it to be inactive.
If a detection rule was disabled or deleted through the Detection Rules page, it is still shown in the Account Takeover tab, but it will not be relevant to the score, regardless of the weight you select.
4. Repeat for other risk factors.

Changes are saved automatically. The risk score calculation will reflect the updated weighting within four hours.

Continuous Identity Discovery

 **Note:** The Continuous Identity Discovery (CID) feature was previously named *Cloud* Identity Discovery.

Introduction

Continuous Identity Discovery (CID) enables you to readily discover privileged identities such as administrator, shadow admin, and service accounts that pose potential security risks. These include accounts that are stale, lacking MFA requirements, or lacking vaulted credentials in Secret Server. CID then prompts you to make specific corrections. CID runs automatically and continuously so you can easily monitor and secure privileged accounts.

CID extends the discovery capabilities of Secret Server Cloud on the Delinea Platform, and represents a subset of the platform [ITP/PCCE](#) (Identity Threat Protection / Privilege Control for Cloud Entitlements) capabilities, including the following:

- **Inventories:** Inventories provide a centralized and comprehensive view of all identities, groups and assets across an organization's cloud services and applications. They offer visibility into privileged accounts based on permissions, roles, groups, and federations. The definitions of privileged accounts and groups are customizable and can be updated as needed.
- **Checks:** Checks enhance IAM hygiene through continuous monitoring of identity misconfigurations and over-privileging by, for example, detecting privileged users and suggesting vaulting for them.


Overview


This overview describes the high-level processes for getting started with CID by establishing a clean, actionable baseline for managing privileged and non-privileged accounts.

Step 1: Add CID Sources

Start by connecting CID to the identity sources you want to monitor. These sources can include Active Directory, Azure AD, AWS, GCP, and more.

1. From the left navigation menu, select **Discovery**.
2. Select **Sources**.
3. Select **Create Source**.
4. On the *Create discovery source* page, select the relevant connectors and configure them with the required permissions

 **Tip:** Adding more sources gives CID a broader view across your environment, improving correlation accuracy.

 **Note:** Once a source is integrated, initial data fetching can take about 24 hours.

Step 2: Review Checks for Non-Vaulted Entities

Once your sources are connected and data fetching completes, CID begins to surface accounts with potential security issues. Begin by reviewing entities that are not yet vaulted, and either vault them or exclude them.

See [Diagnosing Issues with the Checks Panel](#).

Step 3: Establish a Baseline

After vaulting and excluding relevant accounts, you'll be left with a smaller set of accounts that haven't been reviewed yet. These are the undecided cases.

This forms your CID baseline—a clean state where all known accounts are either managed, excluded, or pending review.

Step 4: Customize Privileged User Definitions

With Continuous Identity Discovery, you can update your definitions of administrator and privileged accounts. Use this flexibility to tailor the platform discovery to your organization's specific needs.

CID uses default definitions for *Privileged* and *Admin* accounts. If these doesn't match your organization's standards, you can update them:

1. From the left navigation menu, select **Inventory**.
2. Navigate to **Collections > System**.
3. Modify or create custom system collections that define what constitutes a privileged or admin account

For more details, see [Collections](#).

Step 5: Use Inventory for Advanced Filtering and Reporting

For deeper insights or customized views:

1. From the left navigation menu, select **Inventory**.
2. Select **Identities**.
3. Use filters to view accounts by type, source, vault status, and more.
4. Vault directly from this view or define reports for specific scenarios.

This feature is ideal for compliance audits, scheduled reviews, or identifying gaps in account coverage.

Next Steps

Once you've established your CID baseline:

- Periodically review CID alerts and account recommendations
- Adjust your exclusion and vaulting decisions as systems evolve
- Leverage reporting and filters to monitor for drift or new privileged accounts

Discover Unvaulted Privileged Cloud Service Users

CID Discovery continuously identifies privileged cloud service users that are not yet vaulted in Secret Server Cloud. We recommend vaulting these accounts in Secret Server to enforce proper login, or disabling the user if access is unnecessary.

To discover privileged accounts not managed in Secret Server, select **Identity Posture > Checks** and review the following checks:

- **Unvaulted Admin Credentials**
Discover cloud service administrators whose credentials are not in Secret Server.
- **Unvaulted Shadow Admin Credentials (for CSP only)**
Discover cloud service [shadow admins](#) whose credentials are not in Secret Server.
- **Unvaulted Privileged Account Credentials**
Discover privileged cloud service user accounts whose credentials are not in Secret Server.
- **Unvaulted Admin Access Keys (for AWS only)**
Discover cloud service administrators whose access keys are not in Secret Server.
- **Unvaulted Shadow Admin Access Keys (for AWS only)**
Discover cloud service [shadow admins](#) whose access keys are not in Secret Server.
- **Unvaulted Privileged Account Access Keys (for AWS only)**
Discover privileged cloud service user accounts whose access keys are not in Secret Server.



Note: CID checks identify privileged accounts that are not vaulted based on the provided default templates. Custom templates, however, are not supported. As a result, secrets stored using custom templates may be incorrectly flagged as not vaulted.

Supported Applications

The Delinea Platform currently supports checks for unvaulted privileged accounts, admins, and shadow admins for the following applications:

- Active Directory
- AWS
- Azure
- Entra
- GCP
- Okta
- Snowflake

Discover PAM Bypassing

The Delinea Platform provides a mechanism to detect privileged accounts that bypass Secret Server by logging directly into cloud applications using access keys or login credentials. This detection is based on Identity and Access Management (IAM) activities and involves several checks to identify such bypassing activities.



Status

Included

Description

Admin sync accessed Microsoft Active Directory application using non-vaulted credentials within the past 30 days. Last activity: 2025-01-24 10:58:34 UTC

Recommendation

Vault admin sync log-in credentials in Secret Server

[Vault sync in Secret Server](#)

The PAM bypass detection process involves the following steps:

1. **Activity Collection:** Activities from cloud applications are collected in near real-time. The detection check runs every few hours, allowing results to be available within a few hours. These results are retained for 30 days, after which any detected PAM bypassing alert will automatically resolve.
2. **Comparison with Secret Server:** When a new activity is detected, it is compared with the Secret Server Cloud (SSC) to determine if the account is vaulted. This involves checking the account's activity logs to identify who accessed the applications and whether the account is vaulted.
3. **Check Execution:** To discover cloud privileged accounts bypassing Secret Server, select **Identity Posture > Checks** and review the following checks:
 - **Unvaulted PAM Bypassing Using Access Keys (for AWS only).** Identifies accounts using unvaulted access keys to bypass Secret Server. Alerts are generated if accounts have vaulted access but opt for non-vaulted access.
 - **Unvaulted PAM Bypassing Using Credentials.** Identifies accounts using unvaulted credentials to bypass Secret Server. Alerts are generated if accounts have vaulted access but opt for non-vaulted access.
 - **Vaulted PAM Bypassing Using Access Keys (for AWS only).** Identifies vaulted accounts bypassing Secret Server using access keys, indicating possible use of shared or cached credentials.
 - **Vaulted PAM Bypassing Using Credentials.** Identifies vaulted accounts bypassing Secret Server using credentials, indicating possible use of shared or cached credentials.
4. **Alternative Authentication Methods:** For unvaulted accounts, the system checks if there are alternative authentication methods (such as credentials or access keys) that are vaulted. If such a method exists but the account still logs in using unvaulted credentials, it indicates bypassing of the vaulted authentication method and PAM itself.

Supported Applications

The Delinea Platform currently supports PAM bypass checks for the following applications:

- AWS
- Entra
- Okta
- Snowflake

Discover Delegated Permissions



CID will also discover accounts with delegated administrative permissions, such as delegated permissions for resetting passwords or delegated full permissions within an Organizational Unit (OU).

CID Manual and Bulk Vaulting

Once you have discovered all privileged cloud service accounts in your environment, you can close the loop and vault these accounts in Secret Server Cloud.

You can use manual vaulting or bulk vaulting:

Manual vaulting - You can select a specific account and vault it in Secret Server Cloud using the ellipsis. For more details, see [Creating Secrets](#).



  SHIR

Status
Included



Description
Admin SHIR has access to app Snowflake although it's credentials are not vaulted in Secret Server

Recommendation
Vault admin SHIR credentials in Secret Server



More actions

  NONNA

▼

  ACME

▼

  SAGIV

▼

Bulk vaulting - You can vault all discovered cloud service accounts for a specific application in one click. For a specific checks (see "Discover Unvaulted Privileged Cloud Service Users" on page 739 above):

1. Click the Remediation tab
2. Click the link to vault all accounts in a click of a button
3. The Import modal will open and you will have to fill in some details.

For more details, see [Manually Importing Local Accounts](#).

Detect Shadow Admins Credentials that are not vaulted in Secret Server

Actions



General

Filter Scopes

Affected Entities (3)

Remediation

^ Suggested Steps

Create a secret in Secret Server to enforce proper login or disable the user if the access not needed.

[Vault all # secrets in Secret Server](#) →



Webhooks

No Webhooks

Create a webhook

Create a CID Report

Create a scheduled report to see all privileged accounts that are not vaulted along with additional information about them (account name, source app, privilege type, last login, and more). Using this report you can get all accounts that are not vaulted over time to your email and track remediation progress.

To create a report:

1. Click **Insights** from the left navigation menu.
2. Click **Reporting**.
3. Click **Schedule a Report**.
4. Create a new report with a name, frequency, and email recipients from the type, **Unvaulted Privileged Accounts**.
5. Click **Create**.

Learn more at [Configuring Recurring Reports](#).

Setting Up CID Integrations


For instructions on setting up CID integrations, see the relevant topic:

- [AWS Integration](#)
- [Entra ID and Azure Cloud Integration](#)
- [Okta Integration](#)
- [Ping Integration](#)
- [Snowflake Integration](#)

For more details on [ITP/PCCE](#) capabilities, see the following pages:

- [ITP/PCCE Assets](#)
- [Recurring Reports](#)
- [Identity Posture](#)
- [Threat Center](#)
- [Configuring Risk](#)

Identity Governance Administration

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

On the Delinea Platform, Identity Governance Administration (IGA) helps to secure your organization by managing and controlling user identities, access rights, and compliance requirements. IGA helps to ensure that the correct individuals – whether employees, contractors, or partners – have timely access to the appropriate information, systems, and resources, both physical and digital. IGA also monitors and audits this access, automating management based on your organization's specific configuration. By providing visibility and control, IGA helps prevent unauthorized access, reduces security risks, and ensures compliance with both internal requirements and external regulations.

IGA consists of two critical components:

- **[Identity Lifecycle Management \(ILM\)](#):** Manages the entire lifecycle of user identities, from onboarding to off-boarding, including adjusting access as roles change.
- **[Identity Access Certification \(IAC\)](#):** Ensures secure, role-based access to systems, enforcing policies and governance. (*Note: IAC is not yet available.*)

Current Capabilities


At this time, IGA includes the following capabilities and integrations:

- **Access Management:** Defining who can access specific systems or data
- **[Role-Based Access Control \(RBAC\)](#):** Assigning permissions based on organizational roles
- **Policy Enforcement:** Implementing rules for access, such as approving new accounts or reviewing access rights periodically
- **Compliance:** Ensuring that access-control processes meet regulatory requirements (such as GDPR, HIPAA)

- **Resources / Integrations:** Ping Directory, Okta, Entra ID, as well as physical assets like key cards, ID badges, and printers

For more information, see [Introduction to ILM](#) or [ILM Setup and Configuration](#).

Identity Lifecycle Management

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

On the Delinea Platform, Identity Lifecycle Management (ILM) enables management of users' digital identities across your IT systems, from creation to deactivation – ensuring secure access and compliance while improving efficiency through automation.

For specific system setup and integrations, see [ILM Setup and Configuration](#).

ILM Advantages for Users and Organizations

ILM impacts both organizational security and employee efficiency with the following benefits:

- **Seamless Access:** instant and secure access to the tools and systems needed
- **Improved Security:** protection from unauthorized access and potential data breaches
- **Faster Onboarding:** no delays in getting access to necessary resources when joining a company
- **Frictionless Role Changes:** automatic updates to access when switching teams or getting promoted
- **Self-Service Capabilities:** ability to reset passwords or request access without IT delays
- **Better User Experience:** fewer login issues, less downtime, and a streamlined workflow
- **Compliance & Privacy:** ensures personal and work data are protected and handled securely

Stages: Joiner Mover Leaver (JLM)

ILM operates across three key stages of an identity's lifecycle: Joiner, Mover, and Leaver (JLM). Proper practices at each stage help to ensure that an identity has secure and appropriate access at every stage of its lifecycle.

Joiner

The “Joiner” stage occurs when a new identity is created or added to a system. This identity could represent an employee, contractor, or even non-human identities or hardware.

At this stage, appropriate access permissions must be assigned based on the role of the identity being onboarded.

Mover

The “Mover” stage occurs when an existing identity changes its role. Examples include:

- An employee moves to a new role or department
- A contractor transitioning to a full-time employee.

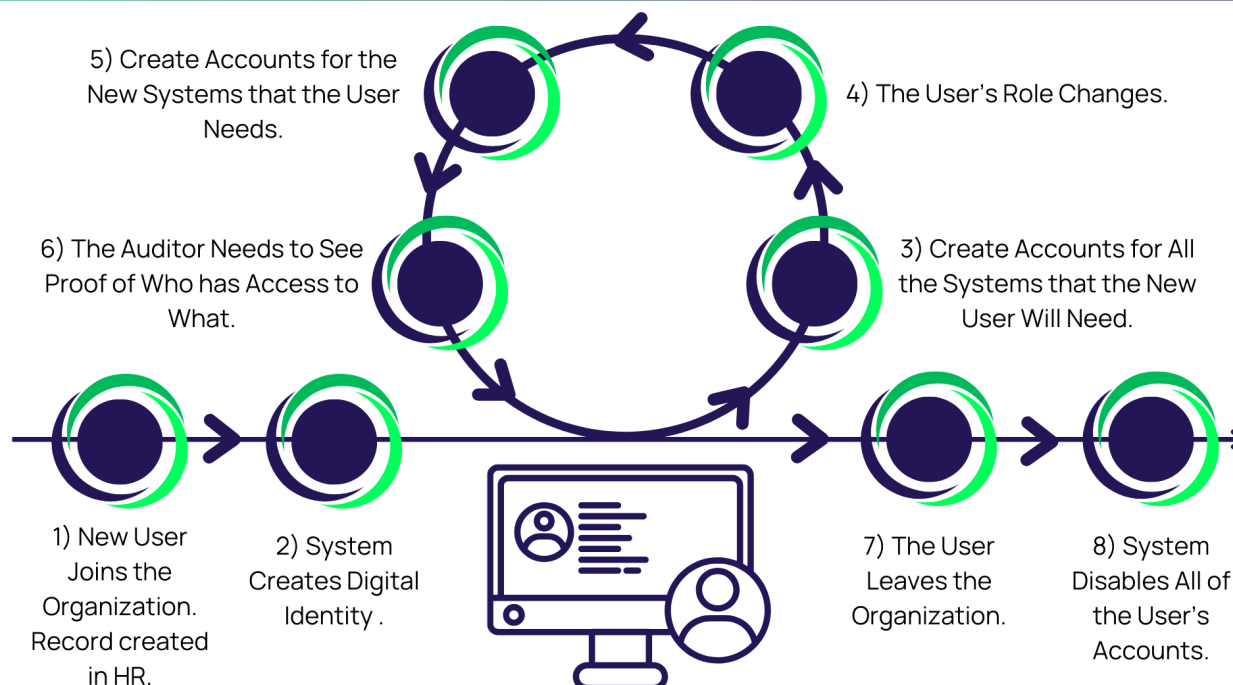
It's important to ensure that only the necessary permissions for the new role are retained, since combining previous access with new permissions can lead to security risks.

Leaver

The “Leaver” stage occurs when an identity is removed from the system, typically upon termination of employment or the end of a contract. Proper ILM operation ensures that all access permissions are revoked, preventing unauthorized access after the individual has left.

Removal of a “Leaver” can be either manual or pre-scheduled (which is ideal for time-bound roles).

Example Identity Lifecycle

Delinea


The image above shows the steps involved in a typical identity lifecycle – in this case for an employee. Lifecycles for different types of users vary somewhat – but the core principles remain the same. The identity lifecycle covers every action that must take place from the moment the individual joins the organization until the moment they leave, including all of the inevitable change that takes place between these two events.

ILM Setup and Configuration


Important: This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

Each organization's systems and identities are unique and there is no one setup process that must be followed for optimal configuration.

The configuration pages below are highly recommended starting points:

- [Delinea Platform Permissions](#): Ensure that your admins have the proper permissions to manage ILM and IGA.
- [User Types](#): Define the various types of users your system will manage.
- [Governance System Settings](#): Set the title of your IGA management team, add an encryption key, and default user type.
- [Data Generation Rules](#): Set powerful rules that ensure consistent, accurate data.
- [Fields](#): Customize data options related to users.
- [Forms and Views](#): Customize the forms and views used for creating and updating users.
- "Resources and Connectors" on page 771: Integrate the digital systems that ILM can grant access to.
- "Roles" on page 773: Define the collection of resources that specific job functions need access to.

User Types

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

Creating and configuring user types is the first step in setting up ILM and IGA. To create, update, or delete a user type, navigate to the **Access** page and select the **User Types** tab.

Access

Roles User Types

Q Search... [Add filter](#)

5 items

NAME ↑	DESCRIPTION	DEFAULT EXPIRATION DAYS	MAX EXPIRATION DAYS	USED
Contractor	Contractor identities		120	Yes
Delinea	User Type for Delinea staff		0	Yes
Employee	Employee user type		0	Yes
NHI - Service Accounts	Non-Human, Service account users		0	No
Vendors	Vendor users		0	No


To create a user type, select **Create** and fill out all required fields, plus any additional ones desired. The table below summarizes field details and requirements.

Field	Required / Optional	Data Type	Note
Name	Required	Unique; Text	
Description	Required	Text	
Enable Email Notification		Boolean	Determines whether an email notification will be sent.
Notify Email Address	Required if Enable Email Notification is true	Text	Email address to notify.

Field	Required / Optional	Data Type	Note
Enable Termination Notification		Boolean	Determines whether a termination notification is sent.
Days Before Termination To Notify	Minimum of one required if Enable Termination Notification is true	Number	The number of days before termination to start the workflow for identity termination notification.
Default Credential Policy	Required	Selection	The default credential policy for this user type.
Default Duration			<p>The default number of days.</p> <ul style="list-style-type: none"> 0 (Zero) indicates unlimited. When both Default Duration and Maximum Duration are set to zero, this user type will not require specification of an end date or duration.
Maximum Duration			<p>The maximum duration allowed.</p> <ul style="list-style-type: none"> 0 (Zero) indicates unlimited. When both Default Duration and Maximum Duration are set to zero, this user type will not require specification of an end date or duration.
Allowed Resources		Multi-Selection	<p>A list of resources this user type can potentially have. Each Resource can be identified as:</p> <ul style="list-style-type: none"> Birthright: All users of this type will be assigned the resource and it cannot be removed. Default Granted: All users of this type are assigned the resource by default, but it can be removed. Default Not Granted: All users of this type are not assigned the resource by default, but it can be added.

Field	Required / Optional	Data Type	Note
Allowed Roles		Multi-Selection	<p>A list of roles this user type can potentially have. Each role can be identified as:</p> <ul style="list-style-type: none"> ▪ Birthright: All users of this type will be assigned the role and it cannot be removed. ▪ Default Granted: All users of this type are assigned the role by default, but it can be removed. ▪ Default Not Granted: All users of this type are not assigned the role by default, but it can be added.

About User Types

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

A user type defines a large grouping of similar users. It can be viewed as a category of users with much in common, even though they don't all have the same business role. Typical examples include staff, contractors, customers, and students.

User types are helpful not only for classifying users but also for provisioning access. One way is by assigning items through birthright access at the user type level.

User types are recommended for grouping users by specific geographies, such as US and UK staff.

About Birthright Access

Birthright access sets the resources, roles, and other things that a particular category of identities get when they are first created.

A common example would be to set Entra ID and Email as birthright resources, since most organizations provision an identity provider account and email address to all staff members, regardless of their job function.

Birthright assignments only manage access to applications, not physical assets.

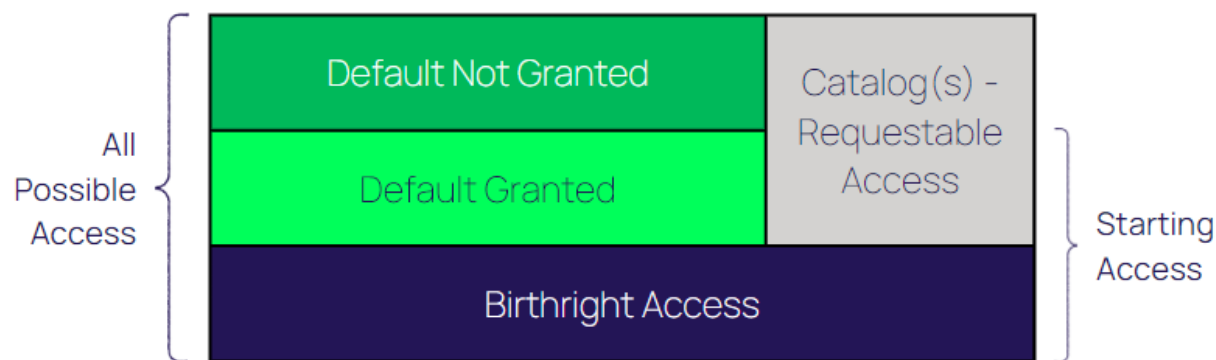
Access Types

- **Resource:** A resource is a digital or physical asset to which a user can be granted access. This could be a physical asset such as a key card or a digital application (Ping Directory, Okta, or Entra ID).
- **Entitlements:** Entitlements are access levels within a resource (security roles, responsibilities, security groups, permission sets, and so forth).
- **Role:** A role is a collection of resources and entitlements. Roles can be assigned to more than one person. Roles are best organized for a specific purpose, such as a specific job function.

Access Model

Every identity has exactly one user type, and this is the foundation of the IGA access model.

Within the user type, administrators configure different access levels for roles and resources (such as birthright, default granted, and default not granted), defining the initial and potential access given to an identity.



Only access defined in the user type can be granted. Anything not explicitly set in the user type can never be granted to an identity of that user type. When access is defined, it is specified in one of the following categories:

- **Birthright:** Birthright access is granted to every identity of this user type and can never be removed.
 - Example: An email account for employees: All identities of the employee user type are granted an email account. They have that email account as long as they are employees.
- **Assigned:** Access is granted to every identity of the user type when the Identity is created or changed to that user type. Access can be removed.
- **Assignable:** Access is not granted to new identities by default. Access can added directly by administrators or managers, by policies attached to a role, or through a self-service request if the access is available in a catalog. Access can be removed.

Ways Access is Granted

Users can obtain access in various ways based on the business processes and security requirements of their organization.

Birthright

Birthright access is access that every identity receives based on their user type. For example, every Delinea employee gets an Azure AD and Slack account. Those would be birthright resources for the “Employee” user type.

Birthright access is granted when an identity is created or updated; however, it is re-evaluated if the user type is updated.

Direct Assignment

An administrator can assign access to an identity; however, only access available to the specific user type can be assigned.

Role Access by Dynamic Collections

Dynamic collections can automatically assign roles to users. A role will be assigned to **all** users in the dynamic collection. Dynamic collections are evaluated:

- When a user is created
- When a user is updated
- On a schedule
- When the collection definition is updated
- When the user type is updated

To view or manage **Dynamic Collections**, navigate to the **Collections** page and select the **Dynamic Collections** tab.

Governance System Settings



Important: This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

The Governance System Settings page offers configurable options that define key operational parameters for ILM. These settings ensure consistency in application behavior, security, and processing logic across the platform.

The three key system settings are:

- "Sensitive Data Encryption (Key Manager)" below
- "Delivery System Time" on the next page
- "Identity Management Settings" on the next page

Sensitive Data Encryption (Key Manager)

You can add a key that encrypts any sensitive data within the ILM system. Only admins with the key will be able to view sensitive data.

To view or edit your Key Manager, navigate to the **Governance System Settings** page, and select the **Sensitive data encryption** tab.

You can view or manage your Encryption Key on this page by clicking **Edit**.

Governance System Settings

Sensitive data encryption

Delivery System Time

Key Manager

Edit

Manage client certificate

Encryption Key

*****3Eo=

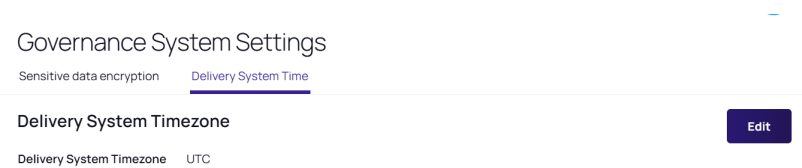
On this page, you can perform the following actions:

- **Eye icon:** You can toggle the visibility of your encryption key by clicking on this icon.
- **Regenerate encryption key:** A new encryption key will be generated.
- **Cancel:** Any changes that were made will not be saved, and you will exit the editor.
- **Save:** All changes that were made will be saved, and you will exit the editor.

Delivery System Time

To view or edit your Delivery System Timezone, from the **Governance System Settings** page, select the **Delivery System Time** tab.

On this page, you can see the currently selected time zone or click **Edit** to change.

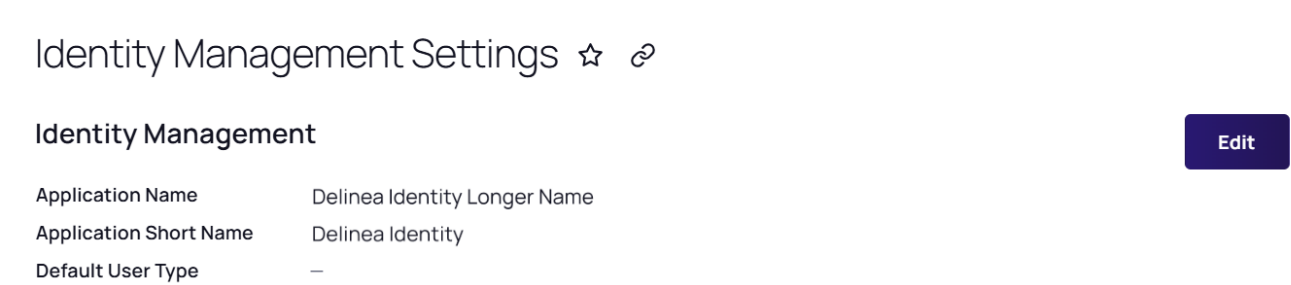


You can select a new time zone from the dropdown list.

Identity Management Settings

The identity management settings define a name for your IGA group (which will be displayed in system emails sent to joiners, movers, and leavers). You can also define the default user type that's created by your IGA system by way of the API (so you don't have to set the user type in the incoming data connector).


To view or edit your Identity Management settings, navigate to the **Identity Management Settings** page.



Click **Edit** to change any of the following settings:

- **Application Name:** This will be the name of the team administering IGA, and may be used in emails sent to identities at various stages of their lifecycle.
- **Application Short Name:** A shortened version of the application name.
- **Default User Type:** If an identity does not have a User Type assigned, the user type selected here will be assigned instead.

Data Generation Rules

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

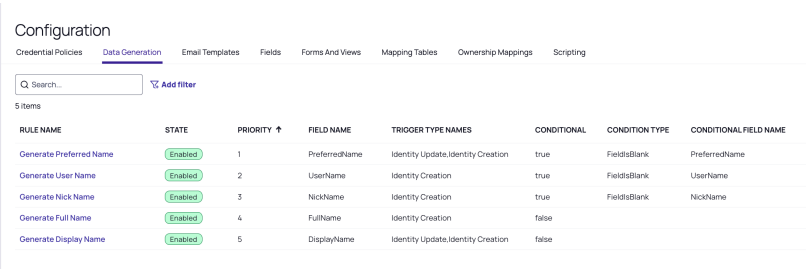
When identities are created or updated, the data added to their fields is governed by data generation rules. Throughout an identity's lifecycle, data generation rules run based on pre-defined triggers.

You can set an order for data generation rules so they will be run in order of priority. If multiple rules have the same priority, they are run in non-deterministic order or in parallel.

For additional details, visit [Data Generation Patterns Syntax](#).

Creating a Data Generation Rule

To view or manage a data generation rule, navigate to the **Configuration** page and select the **Data Generation** tab.



Configuration							
Credential Policies Data Generation Email Templates Fields Forms And Views Mapping Tables Ownership Mappings Scripting							
Q Search... Add filter							
5 items							
RULE NAME	STATE	PRIORITY ↑	FIELD NAME	TRIGGER TYPE NAMES	CONDITIONAL	CONDITION TYPE	CONDITIONAL FIELD NAME
Generate Preferred Name	Enabled	1	PreferredName	Identity Update, Identity Creation	true	FieldsBlank	PreferredName
Generate User Name	Enabled	2	UserName	Identity Creation	true	FieldsBlank	UserName
Generate Nick Name	Enabled	3	NickName	Identity Creation	true	FieldsBlank	NickName
Generate Full Name	Enabled	4	FullName	Identity Creation	false		
Generate Display Name	Enabled	5	DisplayName	Identity Update, Identity Creation	false		

You can select an existing rule to modify or click **Create New**.

Fields

To create a Data Generation Rule, select **Create** and fill out all required fields, plus any additional ones desired. The table below summarizes field details and requirements.

Field	Required / Optional	Data Type	Note
Rule Name	Required	Unique; Text	
Description	Required	Text	If selected, an email will be sent to the specified email address whenever an identity is added to this user type.
Field Name	Required	Selection	The field to which this rule will apply.
Priority			An integer value that defines the priority of this rule relative to other rules.
Enabled		Boolean	If true, the rule is enabled and will be run based on the trigger.

Field	Required / Optional	Data Type	Note
Conditional Rule		Boolean	See "Creating Conditional Rules" on page 756 below.
Triggers		Selection	<p>The selected option defines what triggers this rule to run. Trigger options:</p> <ul style="list-style-type: none"> ▪ Identity Creation ▪ Identity Update ▪ Field Update ▪ Timer<>: <ul style="list-style-type: none"> • Hourly <ul style="list-style-type: none"> ◦ Minute(s) past the hour. • Daily <ul style="list-style-type: none"> ◦ Time of day • Weekly <ul style="list-style-type: none"> ◦ Day of week ◦ Time of day • Monthly <ul style="list-style-type: none"> ◦ Day of month ◦ Time of day
Rule Type		Selection	The type of rule, which can be either script or pattern.
Script		Selection	<p>A script that evaluates the identity to return the value for the field. If this type is selected, then the following fields are required.</p> <ul style="list-style-type: none"> ▪ Script: The script to run.

Field	Required / Optional	Data Type	Note
Pattern			<p>A pattern (or list of patterns) to generate the field's value. If this type is selected, then the following fields are required.</p> <p>Generation Rules:</p> <ul style="list-style-type: none"> ■ Use template strings in the format <code>{{givenname}}</code>, where the template string is any identity field name, including custom fields. ■ In addition, it is possible to restrict the length of the replacement value using the format <code>{{variable:<length>}}</code>, where <code><length></code> is the number of characters you want to use, for example, <code>{{surname:5}}</code> will use five characters from the surname. ■ Spaces can be used. For example, to generate an Identity's full name, the corresponding field can be set to generate data using a format similar to <code>{{honsuffix}} {{givenname}} {{surname}}</code>. ■ These special system template strings are also available: <ul style="list-style-type: none"> • <code>appshortname</code>: The short name of the application • <code>yyyy</code>: The current year as four digits (for example, 2012) • <code>yy</code>: The current year as two digits (for example, 12) • <code>mm</code>: The current month as two digits • <code>dd</code>: The current day as two digits • <code>increment</code>: An incrementing number - if used, must be placed as the last (right-most) string in your rule format. The number of digits can be controlled with the length parameter. For example, <code>*-----</code> will count up to a maximum of 999. ■ When separated by new lines, more than one format can be configured per Rule, and each format will be tried in turn to find a unique value.
Characters to Exclude		Text	<ul style="list-style-type: none"> ■ A list of characters to exclude from the generated value ■ Only available when the field type is a string
Convert to Lower Case		Boolean	<ul style="list-style-type: none"> ■ If true, the field's value will be transformed to lowercase ■ Only available when the field type is a string

Field	Required / Optional	Data Type	Note
Convert to ASCII/Latin1		Boolean	<ul style="list-style-type: none"> If true, the field value will be converted to ASCII/Latin1 character set Only available when the field type is a string
Transform Existing Values		Boolean	<ul style="list-style-type: none"> If true, the field's existing values will be the generation rules' starting point.

Creating Conditional Rules

Conditional rules enable additional adjustments when specific conditions occur, such as a user leaving a field blank.

To create a conditional rule, select the **Conditional Rule** checkbox. Two new dropdown options become available: **Condition Type** and **Conditional Field**.

- Condition Type - Select the criteria that must be met before an action is triggered.
 - Field is blank
 - Field is NOT blank
 - Field equals value
 - Policy is True - If selected, choose a Dynamic Collection.
- Conditional Field - Select the field to be generated if the condition is met.
 - Dynamic Collection will replace this field if the Condition Type is "Policy is True".

For example, if you create a rule to generate a username, and you select the **Condition Type** "Field is blank," and the **Conditional Field** "UserName," and the **Event Trigger** "Identity Creation," then later during identity creation, if the "UserName" field is blank (empty), the system will create a username with this Data Generation Rule. However, if the identity created *does* have a username, the Data Generation Rule will not be triggered.

Mapping Tables

You can configure data generation rules to use a mapping table, to narrow the rule to specific scenarios. To do this, add a lookup to the rule, including the mapping table and the key name.


There are two types of lookups: *by value* or *by reference*.

Lookup Type	Function	Syntax	Note
Lookup By Value	Look up a hard-coded table name and key.	lookup:tableName:key	

Lookup Type	Function	Syntax	Note
Lookup By Reference	Look up a hard-coded table name using a key from the identity data.	lookupRef:tableName:keyField	keyField is the field in the identity record to be used as the key.

 **Note:** Both types of lookup can be used in a single pattern data generation rule; they are not exclusive.

About Data Generation Pattern Syntax

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

A pattern is used to generate data dynamically by grabbing data from entity fields, using lookups (mapping tables), or using keywords like “appshortname” or “increment” to increment for unique fields.

Below, we define general syntax for patterns you can use to generate data.

 **Note:** Fields and values are NOT case-sensitive.

For information on creating and managing a data generation rule, see [Data Generation Rules](#).

General Syntax


Be sure to wrap every substitution with double curly brackets “{}”; otherwise, the literal value will be used to generate the data.

```
{{fieldName}} => grabs value from that field name
Literal value => Literal value
```

Keywords

```
{{appshortname}} => Delinea
{{yyyy}} => 2006 //current date year
{{yy}} => 06 //current date year
{{mm}} => 10 //current date month
{{dd}} => 31 //current date day
```

Field Substitutions

 **Note:** Only the Identity object type is supported at this time, so only identity fields will work. And only Text, LongText fields can be used to generate data.

```
{{fieldName}} => value for field name
{{fieldName[0]}} => value for field name at index 0 (must be an array of string values)
```

Lookup Substitutions

Lookups have three main parts. First, they are prefixed with the keyword “lookup.” Then, they are followed by the mapping table name (spaces must be used if the mapping table name has spaces) and, finally, the row key.



Note: The row key can be followed by an index for mapping tables that have rows with more than one value per row.

`{{lookup.tableName.rowKey}}` => The value for the given mapping table at the given row.
`{{lookup.tableName.rowKey[2]}}` => The value at index 2 for the given mapping table at the given row.

Lookup Reference Substitutions

Lookup references operate the same as lookups in that they can use mapping tables, but instead of providing an explicit row key value, you can use a field on the entity to grab a row key dynamically. They are also prefixed with `lookupref` instead of `lookup`.

`{{lookupref.tableName.fieldName}}` => The value for the given mapping table at the given row. The Row key is generated from the value in `fieldName`.
`{{lookupref.tableName.fieldName[2]}}` => The value at index 2 for the given mapping table at the given row.

Modifiers

This section lists the modifiers that you can add to your syntax to generate values.

Character Length

You can specify the maximum number of characters you want to grab from a field or lookup value.



Note: In the event that the value is less than the provided character length, it will grab the entire value.

`{{fieldName:3}}` => Retrieves only the first 3 characters.
`{{lookup.tableName.rowKey:3}}` => Retrieves only the first 3 characters.
`{{lookup.tableName.fieldName:3}}` => Retrieves only the first 3 characters.

Increment

The number provided with the increment substitution will specify the number of places that will be generated. For example, “1” will start at “1” and increment up to “9”, “2” will start at “01” and increment up to “99”, etc.



Note: This will only increment for fields that have the unique property equal to true.

`{{increment:3}}` => starts at 001 and goes up to 999

Dynamic Collections

Dynamic Collections are policies that evaluate a subject based on a set of rules. The dynamic collection’s object is evaluated as true or false.

For example, if the subject is an identity, the dynamic collection evaluates rules about the identity. If the subject is a resource, the dynamic collection evaluates rules about the Resource.

Dynamic collections are attached to objects or actions in the system to determine if actions should be taken in the system or if access should be granted.

To view or manage a field, navigate to the Configuration page and select the Fields tab. Select Edit or New to manage or create a field.

To view or manage Dynamic Collections, navigate to the **Collections** page and select the **Dynamic Collections** tab.

Q Search

?

☆

🔔

JD

Collections

Static Collections

Dynamic Collections

Q Search...

Add filter

Create Dynamic Collection

2 items

🔍 Name

⌵

🔗

🔄

NAME ↑	DESCRIPTION	SUBJECT	TYPE
All Active Identities	Fastpath default policy for all a...	IDENTITY	Query
Fastpath Administrators (Role-...	The default policy for Fastpath ...	IDENTITY	Query



Note: Hover over the name to display an ellipsis with the options to view, evaluate, or delete the dynamic collection.

Creating a Dynamic Collection

To create a dynamic collection, fill out all of the required and any of the remaining fields:

- **Name** (Required) (Unique) - The name is used as the dynamic collection's identifier.
- **Subject** (Required) - Select the dynamic collection's Subject (this is the type of data you will be working with):
 - Identity
 - Role
 - Resource
- **Description** (Required) - A text description of the dynamic collection
- **Query Scope** (Required) - Use this section to add rules (items) to the ruleset.
 - This section appears only if you select "Ruleset" as the Dynamic Collection Type.
 - At least one rule is required.
 - Rules can be grouped.
 - Logical operators AND or OR connect rules or groups of rules.
 - As each rule is added, the display shows a user-friendly, text-based preview of the rule.
 - Each rule can be negated to evaluate the rule with a logical NOT.
 - The form validates that the rule is valid and displays any errors.

Filling out a Query Scope

Each rule consists of three components - fields, operators, and values.

Field

A field is from the subject data type and it can be any field, including custom fields and the assignment of company, role, entitlement, or resource.

Operator

An operator is based on the data type of the selected field, and based on the field types:

Text Fields	Numeric Fields	Date Fields
Equals	Equals	Before
Not equals	Not equals	After
Contains	Greater than	Between
Starts with	Less than	Exist (has a value)
Ends with	Greater than or equal	Does Not Exist
Is one of	Less than or equal	Relative Date
Does not contain	Is not empty (has a value)	Date (Calendar)
Does not exist	Empty	
Is not like		
Is not one of		
Empty		
Is not empty (has value)		

Value

The value is what the field will be compared to using the operator. It can be a field, literal, or relative value.

Field Value

Another field from the subject type (including custom fields). This field must be of the same type as the comparison field.

Literal Value

A hard-coded literal value of the same data type as the comparison field.

Relative Value

A value that is relative to the field value. A relative value is only applicable to date fields and can be any of the following, where you specify a numeric value for N:

Days	Weeks	Months	Years
N Days Ago	N Weeks Ago	N Months Ago	N Years Ago

Days	Weeks	Months	Years
Today	This Week	This Month	This Year
N Days from Now	N Weeks from Now	N Months from Now	N Years from Now
Yesterday	Last Week	Last Month	Last Year
Last N Days	N Weeks	Last N Months	Last N Years
Tomorrow	Next Week	Next Month	Next Year
Next N Days	Next N Weeks	Next N Months	Next N Years

Deleting a Dynamic Collection

When deleting a dynamic collection, the system checks if it is in use:

- If the dynamic collection is in use, the system notifies the user and they won't be allowed to delete the dynamic collection.
- If the dynamic collection isn't in use, the system deletes it.

Fields



Important: This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

In IGA, fields are components of objects (such as identities, resources, roles, and entitlements). Fields help to constrain data entry, specifying content type, data type, validation requirements, and more.

For more details, see [Understanding Fields](#).

Managing Fields

To view or manage a field, navigate to the **Configuration** page and select the **Fields** tab. Select **Edit** or **New** to manage or create a field.

Configuration

Credential Policies Data Generation Email Templates **Fields** Forms And Views Mapping Tables Ownership Mappings Scripting

 Add filter

162 items

NAME ↑	LABEL	UNIQUE	READ ONLY	FIELD TYPE	DATA TYPE	FIELD OBJECT NAME
AccessUrl	Access URL	Yes	No	System	Text	Resource
active	Active	No	No	System	Boolean	Workflow
Addresses	Addresses	No	No	System	Address	Identity
AllowForcePasswordReset	Allow Force Password Reset	No	No	System	Boolean	CredentialPolicy
AllowPasswordEditing	Allow Password Editing	No	No	System	Boolean	CredentialPolicy
AllowUsernameEditing	Allow Username Editing	No	No	System	Boolean	CredentialPolicy
assignedDate	assigned Date	No	No	System	Date and Time	Workflow Task
assignee	Assignee	No	No	System	Number	Workflow Task
AssignmentPolicyId	Assignment Policy	No	No	System	Lookup	Role
CharacterSetFour	Character Set Four	No	No	System	Text	CredentialPolicy
CharacterSetOne	Character Set One	No	No	System	Text	CredentialPolicy
CharacterSetsToInclude	Character Sets To Include	No	No	System	Number	CredentialPolicy
CharacterSetThree	Character Set Three	No	No	System	Text	CredentialPolicy
CharacterSetTwo	Character Set Two	No	No	System	Text	CredentialPolicy
City	City	No	No	System	Text	Identity Address
Context	Context	No	No	System	Long Text	Identity
Country	Country	No	No	System	Text	Identity Address
CourtesyTitle	Courtesy Title	No	No	System	Text	Identity

Required Fields

If you set a field as required, you can't save the associated [form](#) without entering a value.

Setting a Value

To set a value, use one of the options listed below.

Value Types	Notes
Default Value	This ensures that if the field doesn't have a value, your chosen default value will be used.

Value Types	Notes
Data Generation Rule	<p>This requires that a data generation rule will populate fields when an Identity is created. This is beneficial for fields that are both Required and Unique, since Unique fields cannot have default values.</p> <p>The data generation rule can iterate through possible values using a hierarchical rule-set to generate a unique value and ensure that the required field is populated.</p>
Form Customization	<p>This allows users to add custom fields and values to forms.</p> <p>The Required field must contain a value.</p> <p>A data generation rule or a default value can be used to create a value within the field.</p>

Unique Fields

If you set a field to **Unique**, no other fields of that type may contain the same value. For example, if an identity's `EmployeeNumber` field is set to 120, no other identity can have its `EmployeeNumber` field set to 120. This is because target applications often require uniqueness. Enforcing uniqueness enables centralized data management while meeting downstream requirements.

You can configure [Data Generation Rules](#) to require fields to run through a set of rules. The following process will be applied:

1. If the Field in the Identity is set to Unique, check the result of the uniqueness.
2. If the generated value violates uniqueness, repeat the pattern generation process on the next iteration in the pattern.
3. If there are no more available iterations, go to the next available pattern.
4. If there are no more available patterns, generation will fail.

Creating a Custom Field

To create a custom field, click **Create** and fill out all required fields, plus any additional ones desired. The table below summarizes field details and requirements.

Field	Required / Optional	Data Type	Note
Field Type	Pre-set		Always set to Custom when creating.
Name	Required	Unique; Text	<ul style="list-style-type: none"> ▪ Case sensitive, limited to alphanumeric characters and underscores ▪ No spaces or special characters


Field	Required / Optional	Data Type	Note
Field Object	Required	Select	<ul style="list-style-type: none"> ■ The object type that this field is associated with: identity, resource, role, or entitlement. ■ Only identity fields can be displayed or modified in the UI.
Label	Required	Text	A user-friendly identifier for the field displayed on the UI when it is added to forms.
Data Type	Required	Selection	The type of data stored in the field. See the Data Type table below.
Help Text		Text	Displayed on the UI to provide additional information for the user when filling out a form.
Read-Only		Boolean	If set to true, after the field is created, it can't be updated.
Required		Boolean	<ul style="list-style-type: none"> ■ If a field is required, the object cannot be saved without a value in the field. ■ Making a field required can have severe implications for the system's data flow. For more information, see the "Required Fields" on page 762 section above.
Multi Value		Boolean	<p>Allows more than one value to be contained.</p> <ul style="list-style-type: none"> ■ If set to true, the field will contain a list of the specified data type (cannot be boolean). ■ For example, an Identity might have a custom field called "certifications" listing all the certifications held by that identity.
Unique		Boolean	<ul style="list-style-type: none"> ■ If a field is unique, then only one instance of an object may contain a specific value. ■ Any data type except Boolean ■ For example, if userName is configured as a unique field on Identities, then each identity in the system must have a unique value for userName. If a user with a given userName already exists when another with the same userName is created, then the create will fail to preserve uniqueness. ■ Making a field required can have severe implications for the system's data flow. See the Unique Fields section above for more information.

Field	Required / Optional	Data Type	Note
Default Value(s)		Text	<ul style="list-style-type: none"> ■ This field can have a default value set. The available options depend on the data type. ■ Default values cannot be set on unique fields since that would violate uniqueness.



Note: All Boolean values are set to false by default.

Data Type	Note	Additional Configuration
Text	A free text field of up to 128 characters, displayed as a single line box.	Validation rules – these are enforced on input when possible: <ul style="list-style-type: none"> ■ Maximum Length ■ Validation Regular Expression: A regular expression used to validate the contents of the field when entered.
Long Text	A free text field of up to 1024 characters, displayed as a multi-line text box.	Validation rules – these are enforced on input when possible: <ul style="list-style-type: none"> ■ Maximum Length ■ Validation Regular Expression: A regular expression used to validate the contents of the field when entered.
Date	A date field with no time, displayed as a date picker.	
Time	A time field with no date element, displayed as a time picker.	
Date and Time	A combined Date and Time field displayed as a Date/Time Picker.	
Number	A numeric field displayed as a Number field.	<ul style="list-style-type: none"> ■ Minimum Value ■ Maximum Value

Data Type	Note	Additional Configuration
List Selection	A list of values that can be selected from, displayed as a list selection.	<ul style="list-style-type: none"> ▪ Mapping Table: Select a mapping table to provide a list of key/value choices for the field. ▪ Available Values: A list of field value choices, separated by the pipe character ' '. The field will not pass validation without one of the values provided here, regardless of the field requirement setting. <ul style="list-style-type: none"> •  Note: The user can use the mapping table or available values, not both. ▪ Autocomplete: Whether to auto-complete the field value while typing ▪ Hide Values: Auto-complete fields show a value and a data label; select this option to display the data label only.
Boolean	A boolean value displayed as a check box.	
Lookup	A search option.	

Updating a Field

When updating an existing field, the ability to update its contained fields is changed:

Field Name	Can it be updated?
Field Type	No
Field Object	No
Data Type	Custom fields only
Multi Value	Custom fields only

Deleting a Field


When deleting a field, the system will check if the field being deleted is in use:

- If the field is in use, the user will be notified and won't be allowed to delete the field.
- If the field isn't in use, the field will be deleted.



Note: Only custom field types may be deleted.

About Fields

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

In IGA, fields are components of objects, such as identities, resources, roles, and entitlements. Fields help to constrain data entry, specify content type, data type, validation requirements, and more. In this way, fields serve as the building blocks for [Forms and Views](#).

Fields Enhance Objects

When a field is linked to a specific object type, it allows data input for individual instances of that object type. Fields can describe both intrinsic or “built-in” aspects of an object and any custom extensions defined by users.

For example, an identity object has built-in fields such as “ID,” “username,” “firstName,” and “lastName,” each with pre-defined data types, formats, and validation rules. This built-in field metadata is static and cannot be modified.


Custom Fields

While many pre-defined fields are provided for common data points (user IDs, names, and roles), they may not entirely address your organization's unique requirements.

Customizing fields to your organization's specific needs is critical. By carefully defining relevant fields ahead of time, organizations can ensure data accuracy, improve workflows, and present data in a way that is most useful to their users.

For example, a university might add custom fields like “student ID,” “major,” “graduation date,” or “credits” to an identity object.

Forms and Views

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

Forms and Views are the basic interfaces you define for inputting data to create or update identities.

Managing Forms and Views

To view or manage Forms and Views, navigate to the **Configuration** page and select the **Forms And Views** tab.

Configuration

Credential Policies Data Generation Email Templates Fields **Forms And Views** Mapping Tables Ownership Mappings Scripting

[Add filter](#)



4 items

NAME ↑	FORM TYPE	STATUS	USER TYPE
Create Identity Form	Identity Admin Create	Default	
Identity Display View	Identity Admin View	Default	
Identity Flyout Display View	Identity Flyout	Default	
Update Identity Form	Identity Admin Update	Default	

You can create, update, view, and delete forms and views.

Creating or Updating a Form

To create or update a form, fill out all required fields plus any additional ones desired. The table below summarizes field details and requirements.

Field	Required / Optional	Data Type	Note
Form Type	Required	Selection	<ul style="list-style-type: none"> Choose one of the below forms: <ul style="list-style-type: none"> Identity Flyout Create Identity Update Identity Display Identity  Note: After you've created the form, you can't update the form type.
Name	Required	Unique; Text	
Entity	Required	Selection	<ul style="list-style-type: none"> Currently, Identity is the only option.  Note: After you've created the form, you can't update the Entity type.

Field	Required / Optional	Data Type	Note
User Type	It's not required; however, if no User Type is selected, the form must be either Inactive or Default.		<p>Each user type can have no more than one active form of each form type.</p> <ul style="list-style-type: none"> For example, UserType Employee can only have one active Self-Service Form Type.
Status			<p>Active, Inactive, or Default.</p> <ul style="list-style-type: none"> Each form type can have no more than one default form. The default form cannot be assigned to a user type. There must always be exactly one default for the form types below. <ul style="list-style-type: none"> Create Identity Form Update Identity Form Display Identity Form If the currently created form is set to default, the existing default of the same type will automatically be set to Inactive.

Deleting a Form

When deleting a form, the system will check if the form being deleted is the default for any of the below types:

- Create Identity Form
- Update Identity Form
- Display Identity Form

If it's the default, you won't be allowed to delete the form. If it's not the default, the form will be deleted.

Using the Create Identity Form

The Create Identity form is accessed by administrators and/or managers.

Fixed Values

The fixed values section lets you specify the fields that will have fixed values for all users of the form.

Fixed values might not be displayed to the end user, but they are passed on to every Identity object they create.


Fields

The fields section lets you specify the fields displayed on the form.

In addition to the maximum of five selectable sections, the user may include the following pre-configured sections:

Field	Required / Optional	Data Type	Note
Roles		Boolean	Allow roles to be viewed and configured for the user.
Resources and Entitlements		Boolean	Allows resources and entitlements to be viewed and configured for the user.

About Forms and Views

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.


In IGA, forms and views enable viewing and updating data in Identities. Basic forms enable the following actions:

- **Identity Creation:** Create identities in the system.
- **Identity Update:** Update existing identities in the system.
- **Identity Displays:** View existing identities in the system.
- **Identity Flyouts:** Get a quick view of additional information on existing identities on the Identities Inventory page.


Customizing a form can help to capture additional data needed for managing identities.

Forms and User Types

The user type defines what is included on basic forms. You can use default forms, or customize them for your needs. You can also designate alternate forms as the default.

 **Note:** There can be only one default form for each form type.


You can also create a custom form and associate it with a user type. A form associated with a user type will be used for the user type's identities instead of the default form.

 **Note:** A form can be associated with multiple user types, but each user type can only have one form associated with it.

When selecting a form to display, consider the following:

1. Determine what user type is being created or updated.
2. If there is a form that is associated with that user type, use that form.
3. If no form is associated with that user type, use the default form.
4. If no default form is available and no forms are available for the given user type, then creating and updating identities of that type through the UI is not allowed.

Resources and Connectors

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

To implement IGA and ILM, you must integrate the Delinea Platform with your workforce management system (such as BambooHR or Workday) and / or your identity and access management system (such as Entra ID or Okta). In Delinea IGA these applications are called resources. You can associate a resource with an identity, so that creation of a new job role in the HR system automatically creates an Entra ID account and email address for this person.

Available Resources / Connectors (Coming Soon)


- BambooHR Connector
- Entra ID Connector
- Okta Connector
- PingOne Connector
- Workday Connector

Managing Resources

To view, create, or edit a resource, navigate to the **Resources** page.

Resources

Resources are the applications and physical assets in your organization that can be requested by an identity or assigned to an identity.



 Add filter Create Resource

3 items ⌵ Name ⌵ ⌵ ⌵


NAME ↑	FRIENDLY NAME	DESCRIPTION	USED	ENTITLEMENTS
BambooHR	Bamboo HR	Bamboo HR is the autho...	No	0
BizApp	Business Application	This is an important bus...	No	0
Delinea IGA		Default Delinea IGA Res...	Yes	9

Creating a Resource

To create a resource, select the Create Resource button. On the resulting page, fill out all of the required fields and any additional desire fields (referring to the below table) and select **Save**.

Field	Required / Optional	Data Type	Note
Name	Required	Unique; Text	A unique name for the Resource.
Friendly Name		Unique; Text	An optional, more legible and memorable name for the resource.
Description	Required		A text description of the Resource.
Email Message		Text	If provided, the text entered here will be included in the email sent to the user when the resource is assigned.
Label		Selection	A simple tag applied to a resource.
Application		Boolean	If set to true, this resource will be an application.
Integration		Selection	<p>Select an integration from the dropdown list.</p> <ul style="list-style-type: none">  Note: The “Integration Settings” section and the “Supported Objects” and “Action on Resource Removal” fields only appear once an Integration is selected.
Supported Objects		Lookup; Selection	<p>Select users and/or groups. This will define what will be available for synchronization and provisioning through this integration.</p> <ul style="list-style-type: none">  Note: If the integration only supports one object type, then only that type will be displayed here.
Action on Resource Removal			<p>Defines what the IGA system does when a user loses access to this resource.</p> <ul style="list-style-type: none"> Delete: When a user loses access to this resource, their account in the integrated system will be deleted. Disable: When a user loses access to this resource, their account in the integrated system will be disabled.

Access Requests

- **Auto Approved:** Allows identities to add this resource to their account instead of initiating a request, which will have to go through an approval process.
 -  **Note:** If this field is set to true, you can't configure the Owner field.
- **Owner:** Once an Owner is added, the selection can be edited or removed only until the resource is saved.

- **Request Reason Required:** When set to true, identities cannot request this role unless they provide a reason to accompany their request. When set to false, providing a reason when making a request is optional.

Workflows

- **Approval Workflow:** The workflow to run to approve access requests to this resource
- **Added Workflow:** The workflow to run when this resource is added to a user
- **Removed Workflow:** The workflow to run when this resource is removed from a user

Deleting a Resource

When deleting a resource, the system will check if the resource being deleted is in use.

- If it is in use, you will be notified and won't be allowed to delete the resource.
- If it is not in use, the resource will be deleted alongside any related entitlements.

A resource is considered in use if it is:

- Assigned to any identity
- Part of any role
- In any catalog
- Assigned to a user type

Roles



Important: This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

A role is a collection of resources and entitlements that can be assigned to new identities with similar access needs. Roles should be created with the basic access required for a specific job or function.

To view or manage a role, navigate to the **Access** page and select the **Roles** tab.

Access ☆ ↻

Roles User Types

Q Search...

Add filter

Create Role

9 items


↑ Name ⌵ ⌵ ⌵ ⌵

NAME ↑	DESCRIPTION	USED
Campaign Administrator	Manage and schedule campaigns in Certifi...	Yes
Campaign Reviewer	Perform campaign reviews and execute ca...	Yes
Certification Administrator	Administration access to manage Certifica...	Yes
Certification Auditor	View-only access to certification campaig...	Yes
Fastpath Administrator	Grants complete administrative control, pr...	Yes
Identity Administrator	Administration access to manage resourc...	Yes
Identity Auditor	View-only access to identity & user access...	Yes

Creating a Role

To create a role, select **Create** and fill out all required fields, plus any additional ones desired. The table below summarizes field details and requirements.

Field	Required / Optional	Data Type	Note
Role Name	Required	Unique; Text	The name is used as the role’s identifier.
Description	Required	Text	A text description of the role.
Manager		Lookup	Role Manager. This manager will be considered a secondary manager for any identities assigned to this role.
Is Auto Approved		Boolean	<div><div>▪ Allows identities to add this role to their account instead of initiating a request, which will have to go through an approval process.</div><div><div></div><div>Note: If this field is set to true, the Owner and Owner Type fields cannot be configured.</div></div></div>

Owner Type		Selection	<ul style="list-style-type: none"> Select an identity or identity collection.  Note: Selecting an owner type will allow you to select an owner.
Owner		Lookup	Once an owner is added, the selection can be edited or removed only until the role is saved.
Reason Is Mandatory		Boolean	When set to true, identities cannot request this role unless they provide a reason to accompany their request. When set to false, providing a reason when making a request is optional.
Assignment Collection		Selection	A policy that, when true, assigns this role.
Resources		Lookup	Resources assigned to this role.
Entitlements		Lookup	For each resource, any entitlements that are also granted by this role.

Updating a Role

The table below shows the editing limitations of an existing role.

Role Name	Limitations
Is Auto Approved	Cannot be updated
Owner Type	Cannot be updated
Owner	Cannot be updated

Deleting a Role

When deleting a role, the system will check if the role being deleted is in use:

- If the role is in use, you will be notified and won't be allowed to delete the role.
- If the role is not in use, it will be deleted.

Roles and Access



Important: This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

Role-Based Access Control (RBAC) is a foundational element of Identity Governance Administration (IGA), associating an identity's role (for example: student, administrator, auditor) with their permissions or levels of access to an organization's IT systems, software, and data.

Roles group specific resources (applications) and entitlements to simplify and standardize access management.

Example: A writing application may have a "Writer" role that allows users to edit and delete articles and a "Reader" role that only allows users to read articles.

By grouping resources and entitlements into roles, RBAC streamlines the access assignment process, making it easier to provision, manage, and revoke access as users join, move within, or leave the organization.

Scenarios without RBAC

Working without RBAC might be acceptable for a small organization, but can rapidly create get out of hand and cause administrative challenges.

Consider a scenario where there are *no* roles defined. When a request for a new account comes in, the person creating the account must decide what level and type of access to grant, perhaps by:

- asking the new user's manager (in the hope that they know)
- granting the same access as someone else in the same department or with the same job (though you we don't know if that person has the right level of access)
- giving them access to everything (which happens more than you might think)

None of these scenarios is ideal, and can quickly lead to access sprawl, creating significant problems with:

- Security – because users may have more access than they need, and administrators have no real way of knowing.
- Efficiency – because time and effort are expended trying to determine what access to provide what access someone actually has (for mandatory audits).

RBAC enables you to understand the varied access requirements across your organization, and helps prevent access from becoming a "free for all."

Benefits of RBAC

An RBAC-based approach to access offers many advantages, including eliminating guesswork when making access decisions.

A well-defined RBAC model will specify exactly what level of access each role within the organization should have. The IT administrator doesn't need to know all the details – only which role the user has, and the rest will follow automatically.

Even better, you can synchronize role information from an authoritative source which automates the whole process end-to-end. If your HR system is the authoritative source, you can synchronize an identity's job role from HR and map it to a role in RBAC.

Example: a new user is created in the HR system with a job role of 'Financial Controller' and they are automatically granted appropriate access to QuickBooks and Salesforce.

Connecting to Secret Server Cloud

On the Delinea Platform, secrets work the same way they do in Secret Server Cloud.

When Secret Server Cloud and the Delinea Platform are integrated, the two systems share secrets and pinned folders, as well as administrative privileges, permissions, and access settings.

[Integrate Using Platform Integration Center](#) is the easiest way for existing Secret Server Cloud customers to integrate their tenant into the Delinea Platform. The Platform Integration Center is currently available only as a private preview. If you wish to participate in this private preview, please contact your Delinea account team or Delinea support for details. Customers using Entra or OpenLDAP in Secret Server cannot currently use the Platform Integration Center.


[Integrate Using Opt In](#): If you do not or cannot participate in the Platform Integration Center private preview, you can opt-in to automatic integration with the Delinea Platform. You will gain Platform Administrator privileges while retaining all of your existing Secret Server Cloud administrator privileges. You will not gain any new Secret Server Cloud administrator privileges.


[Integrate Manually](#). A very small number of customers might need to manually integrate Secret Server Cloud.

Adding Privileged Remote Access to Secret Server On Premises

[Connecting to Secret Server On Premise](#): The integration of Secret Server On Premise with the Delinea Platform is currently limited to the [Remote Access](#) use case only. To use this integration, you must launch a Remote Access session from a vaulted secret stored in Secret Server On Premise. No secret server capabilities, such as lifecycle management, can be managed from the platform interface at this time.

Using Platform Integration Center

 **Important:** This feature is currently available only to customers participating in a Private Preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

 **Important:** The seven steps below correspond to a [walk-through demonstration](#) of the Platform Integration Center. We recommend walking through the demonstration as you complete these tasks.

Overview

This documentation is for customers who are already using Secret Server Cloud who wish to integrate their Secret Server Cloud instance into the expanded capabilities provided by the Delinea Platform

Integration Benefits

The Delinea Platform seamlessly extends privileged access management across your company's hybrid, multi-cloud infrastructure, with adaptive controls that help IT and cybersecurity teams to rapidly meet compliance and reduce risk. The Delinea Platform delivers a multitude of benefits, including:

- **Decrease Risk:** Enhance your security posture by safeguarding privileged access from login to privilege elevation and proactively address identity-related threats and misconfigurations.
- **More Easily Meet Compliance:** Adaptive authorization controls and unified auditing simplify the enforcement and demonstration of compliance requirements.
- **Centralize Control:** Manage privileged access across shared credentials and all identities spanning data, applications, cloud, and traditional infrastructure.
- **Scale Your PAM Program:** Leverage the Delinea secure cloud-native architecture to mature your organization through the seamless adoption of privilege controls and shared capabilities.
- **Realize Fast ROI:** Benefit from wizard-driven setup, configuration, and workflows that are easy to adopt.
- **Benefit from Cloud-Native Resilience:** Experience the most resilient solution, boasting 99.99% uptime.

Learn more about the [Delinea Platform](#) and its shared service capabilities.

After Integration

What Changes

Once the integration is complete, the platform and Secret Server run with unified administration. Management of roles and permissions transfers completely to the platform, and they become read only in Secret Server.

What Stays the Same

When Secret Server and the Delinea Platform are integrated, secrets work the same way on the platform that they always worked on Secret Server. The integrated systems share secrets and pinned folders, as well as administrative privileges, permissions, and access settings.

Secret Server Cloud customers keep everything they know and use today with no disruption to their secrets, workflows, files, or permissions.

- All your secrets, data, and permissions, remain intact and accessible
- There will be no downtime or disruption to service when you opt-in and move identity to Platform
- All your integrations remain configured
- All your customization remains intact
- You will notice very few UI differences
- All historical data and audit trails remain visible
- You keep all functionality and features you currently have
- Your current SLA remains in effect and intact

Have users log on early



Note: Users will not appear on the platform's list of users until they log onto the platform for the first time. We strongly recommend having all users log on to the platform to access Secret Server soon after the integration.

Here is a useful demonstration showing how users can [log on to the Delinea Platform and access Secret Server](#).

Integration Steps

In Secret Server Cloud, launch the **Platform Integration Center**:

1. Click **Settings** from the left navigation menu.
2. Navigate to **Secret Server > Platform Integration > Integration Center**.
3. Optional: Click the star to add the Platform Integration Center as a favorite for ease of access.



Important: The seven steps below correspond to a [walk-through demonstration](#) of the Platform Integration Center. We recommend walking through the demonstration as you complete these tasks.

Step 1: Provision a Platform Tenant

In this step, you will create a new Delinea Platform Tenant and login. This step is required before proceeding to the next step.

For additional information, please see [Integrate Using Opt In](#).

During this process, you will provide a tenant name that is typically the same as your Secret Server Cloud tenant name. For example, if Secret Server Cloud is named **Alpha1.secretservercloud.com**, then your Platform tenant would be named **Alpha1.delinea.app**.

The default region will match your Secret Server Cloud Region. If it is the United States (US), then platform will also be hosted on the US Cloud.

Once the Tenant setup is complete, click **Launch Platform**. The process will automatically log you on to the Delinea Platform where you will be asked to update the account password for the cloudadmin account. Please remember the password you have set.

Launch the **Platform Integration Center** from the platform this time:

1. Click **Settings** from the left navigation menu.
2. Navigate to **Secret Server > Platform Integration > Integration Center** where you can begin Step 2: Secure Access.



Note: The initial platform administrator is named cloudadmin@[tenantname] and all processes described in this document must be completed by that cloudadmin user. The cloudadmin will get the same secret server permissions as the user provisioning the platform tenant. On the Delinea Platform they will get additional permissions as a Platform Administrator.

Step 2: Secure Access

On the Platform, user security and log-in configurations are managed by [Identity Policies](#). If you configure one or more Active Directories using the Delinea Connector, we strongly recommend implementing an Allow List identity

policy. Although a default policy provides baseline configuration, you should tailor it to your organizational requirements.

In Step 2: Secure Access, you will configure the platform for allow-list authentication, similar to existing Secret Server behavior.

The steps below configure an Allow List identity policy that mirrors the default policy but is scoped to a specific group membership so that only the specified users can meet the profile. They then set the default policy to deny access to any users who do not meet the new profile that is configured.

For more details about these settings, see [Identity Policies](#).

If this policy is not created automatically during this step, you can manually create a new Identity Policy by following the steps below.

1. From the platform, click **Access** from the left navigation , then click **Groups**.
2. Create a new group.
3. Name the group to indicate that it defines all users who can authenticate to the platform, such as *Acme Platform Users*.
4. Add the cloudadmin user to the group
5. Add any other users that are currently using the platform to the group, either directly or by a group that they are a member of.
6. Click **Access** from the left navigation , then click **Identity Policies**.
7. Add a new policy.
8. Name the policy to indicate that it will control how most users authenticate to the platform, such as *Acme Default Authentication Policy*.
9. Leave the policy disabled.
10. Add a description if desired.
11. Target specific groups, and select the group that was configured above.
12. In the new policy, click the **Authentication** tab.
13. Edit the **Services** section.
 - a. Enable authentication policy controls.
 - b. Set the **Default Authentication Profile** to **Default Other Login Profile**.
 - c. Save the section.
14. Edit the **Authentication Rules** section.
 - a. Add a rule named, *Identity cookie is not present*.
 - b. Select the **Default New Device Login Profile**.
 - c. Add a filter by selecting **Identity Cookie** and setting **Is not present** for the condition.
 - d. Save the filter, rule and section.

If saving any of these settings causes an error:

Adding Privileged Remote Access to Secret Server On Premises

- Ensure that all steps above have been completed correctly,
 - Ensure that the cloudadmin user can meet the requirements of the two authentication profiles configured above.
15. Open the **Overview** tab and enable the policy.
 16. Navigate back to **Identity Policies**.
 17. Edit the default policy.
 18. Open the **Authentication** tab and edit the **Authentication rules** section.
 19. Select the row and delete any authentication rules.
 20. Save the section.
 21. Edit the **Services** section.
 22. Set the **Default Authentication Profile** to **Deny platform authentication**.
 23. Save the section.

Step 3: Customize Branding

In this step you will configure the platform's look and feel and to comply with organizational expectations.

If your current Secret Server Cloud tenant has branding customizations, this step will copy those branding customizations to your Delinea Platform tenant.

If you have any branding customizations already in the Delinea Platform, there are no actions needed for this step and it will be marked as such.

If you do not have any branding customizations and none are detected, you can skip this step.

Step 4: Connect Domains

In this step, you will Install a Delinea Connector in each forest containing any Active Directory domain(s) currently synchronized with Secret Server.

Basic Requirements for "Installing the Delinea Connector" on page 272:

- Windows Server 2019 or newer
- No outbound SSL inspection
- Domain-joined to a domain in the forest

Please Note:

- Provision an appropriate server to run the connector. The same server that is running the Distributed Engine can be used, but the minimum requirements will differ.
- Directory integration on the platform works slightly differently than in Secret Server and creates a connection to the directory for live querying on demand.
- The connector must be configured to migrate Active Directory users or groups for each forest from which Secret Server users are synchronized.

Adding Privileged Remote Access to Secret Server On Premises

- If you do not have any AD Domains configured in Secret Server, this step will automatically be completed and show the message, *No Active Directory Domains configured in Secret Server and no connectors are required.*

Step 5: Set up Federation

In this step you will configure your federation providers for single sign-on.

Federation is configured much per any other application, there are guides for some popular IdPs available in [SAML and OIDC Federation](#).

- If Secret Server currently has Active Directory users, and this Federation source is intended for logging them in, set the mapping option to **Required** and ensure that **Create local user if unable to map** is *disabled*. These settings prevent a user from being logged in unless they exist in the domain, and ensure that the platform has access to all the associated data, like group membership and enabled state.
- If this Federation source is intended for users that are not currently associated with a domain in Secret Server, set the mapping option to **Required** and ensure that **Create local user if unable to map** is *enabled*. These settings will create all users as Delinea Directory users, as opposed to Federated Directory users, which assists with the migration process.
- Add any UPN suffixes or login domains to the list of domains at the bottom of the federation configuration. This determines which usernames will trigger redirection to this IdP, and which domain connectors are used for finding domain users.

Step 6: Data Pre-check

Check and synchronize Secret Server users, groups, and roles into the Delinea Platform Identity Store.

The integration center is used to move the required data for the Platform to correctly associate, map, and authenticate local users to facilitate an enhanced experience when logging into the Delinea Platform. When targeting Local Groups for migration, the following data will be copied into the Platform Identity Service:

Secret Server Roles

All roles that exist within Secret Server will be copied into the platform database, pre-pended with *Secret Server*. For example, the **Administrator** built-in role in Secret Server will be copied into the **Secret Server Administrator** role on the platform.

Local Users

Users will be copied from Secret Server Cloud into the Platform, including the password hash, enabling them to login to the platform directly with their existing Secret Server username and password.

Local Groups

New platform groups will be created with the same name as the existing Secret Server groups, and the membership will be updated to reflect the membership in Secret Server. These groups will be set to **Managed by platform** and will become read-only in Secret Server.

Associations Between Local Groups and Domain Users with the Delinea Connector

All domain users that belong to migrated groups will be looked up in the domain via the Delinea Connector, and an association will be made to the user in Secret Server such that when Secret Server needs information about the user, it can request it from the Platform. Once the user logs in, the Platform will associate them with the group.

Associations Between Local Groups and Secret Server Roles

Any Secret Server group selected for migration will become a member of the Platform role associated with the Secret Server role attached to the Secret Server group. For example, the **Break-Glass Admins** group that is currently a member of the **Administrator** role in Secret Server would become a member of the platform's **Secret Server Administrator** role.

Before and after migrating a group, the users and groups will remain unchanged in Secret Server, aside from the new metadata that provides information on looking those objects up in the Platform.

At this point, users can authenticate to either Secret Server or the Delinea Platform, and have equivalent access and experience aside from some UI differences between the two applications.

We recommend migrating a small number of users first and validating the process and the user functionality described above, before migrating larger batches through to completion.

Step 7: Complete the Integration

This is the final step for unifying management after all local users, groups, roles and permissions have been copied over (migrated) to the Delinea Platform.

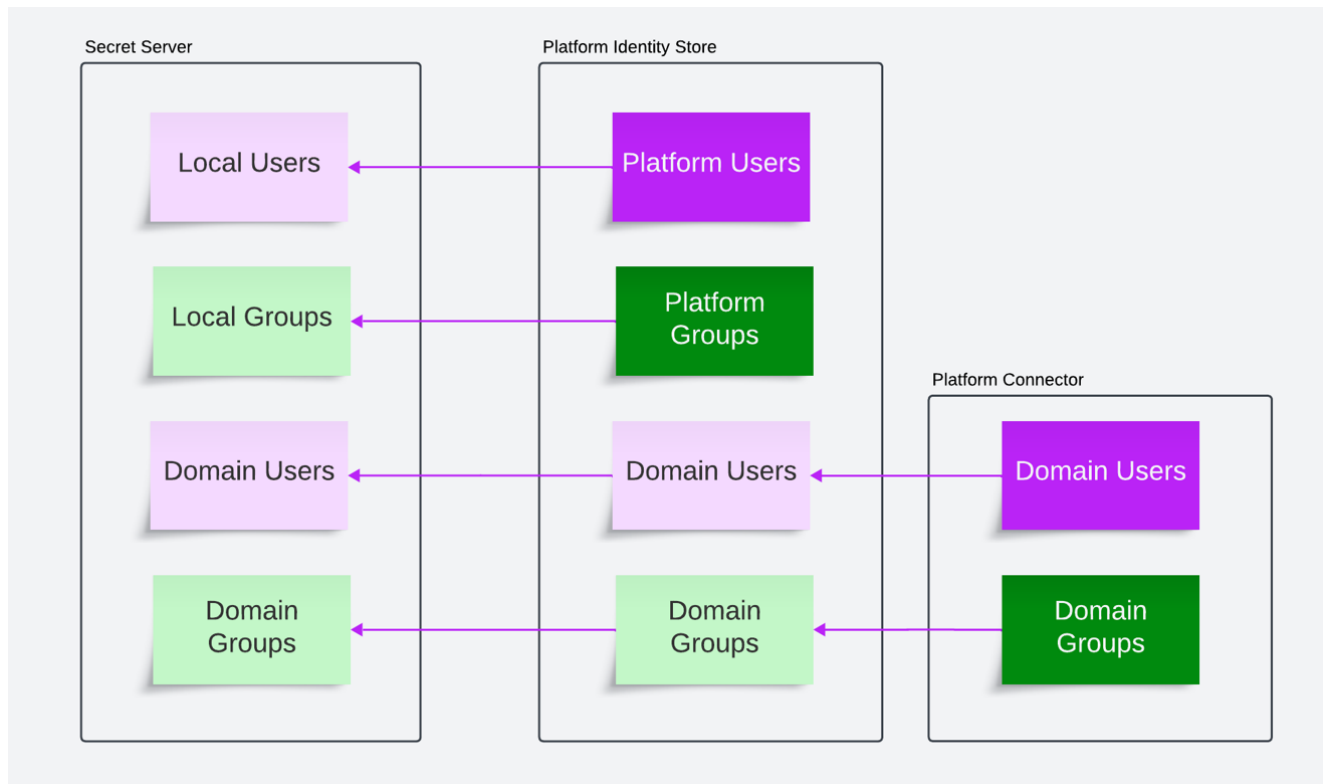
In this step, you will transfer management of roles and permissions to the Delinea Platform as the authority.

Role and Permissions management in Secret Server will change to read only.

Users and Groups are fully orchestrated by the Platform and any updates to the platform objects (user details, membership changes etc.) will be reflected in Secret Server.

The diagram below shows the information flow once this step is completed.

Adding Privileged Remote Access to Secret Server On Premises



After this step is implemented, we strongly recommend having all users log in via the Delinea Platform and access Secret Server. See this [demonstration](#).

Now that you are fully integrated into the [Delinea Platform](#) you can leverage other applications such as.

- [Privileged Remote Access](#)
- [Privilege Control for Servers](#)
- [Identity Threat Protections and Privilege Control for Cloud Entitlements](#)
- "Continuous Identity Discovery" on page 738
- "Integrations and Marketplace" on page 587
- [NextGen Mobile Application](#)

Welcome to the next generation Delinea Platform.

More useful links:

- [Delinea Platform Documentation](#)
- [Delinea Platform API Documentation](#)
- [Configuring Duo Authentication](#)

Using Opt In Integration

This page tells how to take advantage of an automatic process for integrating a new platform tenant with your existing Secret Server Cloud.

Automated Platform and Secret Server Cloud Integration

The procedure to integrate the Delinea Platform and Secret Server Cloud depends on whether you are a new customer or a current Secret Server customer.

New Delinea Customers

If you are a new Delinea Platform customer, the platform comes with built-in, pre-integrated Secret Server functionality, so you will not need to perform any integration steps. You can disregard the rest of the instructions on this page.

Current Secret Server Customers

If you are already a Secret Server administrator, you may be able to opt in to a process that provisions a new platform tenant for you and integrates it with your Secret Server Cloud instance.

This process automatically provisions a new platform tenant and integrates it with your Secret Server Cloud instance. The integration is seamless and harmless to the current operations of your existing Secret Server Cloud instance.

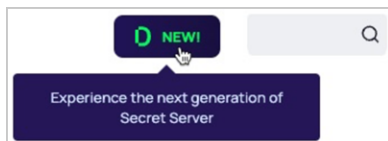
Once you are in your platform tenant, all the Secret Server capabilities are provided, including secret lifecycle management, reporting, inbox, and administration.



Note: Existing Secret Server administrators who become Delinea Platform administrators through the "Opt-in" mechanism retain all their existing Secret Server administrator privileges (but gain no new SS privileges) and automatically gain Delinea Platform administrator privileges.

To get started:

1. Log in to your Secret Server Cloud instance as a tenant administrator with platform integration permissions.
2. Near the top of the portal, click the **New!** button.



If you do not see the **New!** button, you can still provision a platform tenant by contacting your Delinea representative or by completing the steps below:

1. Browse to `<tenant>.secretservercloud.com/ConfigurationAdvanced.aspx`
2. Edit the configuration, and set the "Delinea Platform Enablement Code" to BETTERTOGETHER.
3. Save the configuration.
4. Go back to the Secret Server home page.
5. Click the "New!" button at the top near the search bar.
6. Follow the guide, entering a tenant name and initial admin email address.
7. Access the tenant through the link in the browser or in the invitation email sent to the initial admin email address.
8. Set a password for the `cloudadmin@<tenant>` account.

Adding Privileged Remote Access to Secret Server On Premises

The **Delinea Platform Setup** wizard appears. *Step 1* provides a brief introduction and some platform benefit highlights.

The screenshot shows the 'Delinea Platform Setup' wizard at Step 1, 'Introduction'. A progress bar at the top shows three steps: 1 (Introduction, active), 2 (Delinea Platform Setup), and 3 (Create Tenant). The main content area includes a heading 'Experience the Next Generation of Secret Server!', a paragraph about the next generation of Secret Server, and a section titled 'The Delinea Platform Benefits' with four bullet points: launching secure VPN-less sessions, seamless integrations, secure authentication methods, and discovering integrations in the Delinea Marketplace. At the bottom right are 'Cancel' and 'Proceed' buttons.


3. Click **Proceed**.
4. In *Step 2*, verify that the pre-populated information is correct, and update it if necessary.

The screenshot shows the 'Delinea Platform Setup' wizard at Step 2, 'Enter Your Delinea Tenant Information'. The progress bar shows Step 2 is active. The form contains several sections: 'Create Platform Tenant' with 'Tenant Name' (pre-filled with 'tenant') and 'Platform Region' (pre-filled with 'US'); 'Create Initial Platform Administrator' with 'Platform Admin Username' (pre-filled with 'cloudadmin@tenant'), 'Platform Admin Password' (pre-filled with 'Set upon initial login'), and 'Platform Admin Email' (pre-filled with 'Administrator@company.com'); and 'Connect Platform to Secret Server' with 'Secret Server URL' (pre-filled with 'theotest.secretservercloud.com'). At the bottom are 'Back', 'Cancel', and 'Next' buttons.

All fields are pre-populated and some cannot be changed:

- **Tenant Name:** *Editable*. Contains the characters that precede **.secretservercloud.com** in your existing Secret Server Cloud tenant URL. Although this field is editable, we recommend accepting the default provided.
- **Platform Region:** *Editable*. Select the region that most closely matches where your Secret Server instance is located. Available Regions: US, EU, UK, Canada, Southeast Asia, and Australia.

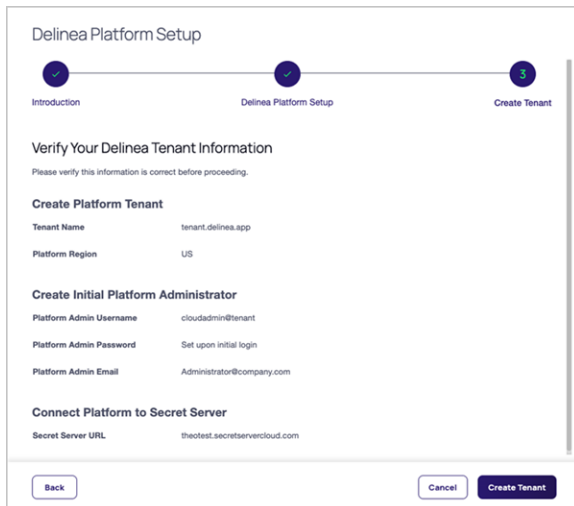
Adding Privileged Remote Access to Secret Server On Premises

 **Note:** The EU region for Secret Server Cloud is in a different location from the EU region for the Delinea Platform. For more information, see [Hosting Regions](#).

- **Platform Admin Username:** *Not editable*. The Platform Admin Username is different from your Secret Server Cloud username. It represents the platform admin user account that will be created on the Delinea Platform.
- **Platform Admin Password:** *Not editable*. It is set upon initial login.
- **Platform Admin Email:** *Editable*. Contains your email address from Secret Server. You can change this address if desired. The email address in this field becomes a part of your platform login credentials, and it is where you will receive your Delinea Platform confirmation email.
- **Secret Server URL:** *Not editable*.

5. Click **Next**.

6. In *Step 3*, verify that the information provided is accurate and click **Create Tenant**.



Delinea Platform Setup

Introduction Delinea Platform Setup Create Tenant

Verify Your Delinea Tenant Information

Please verify this information is correct before proceeding.

Create Platform Tenant

Tenant Name tenant.delinea.app

Platform Region US

Create Initial Platform Administrator

Platform Admin Username cloudadmin@tenant

Platform Admin Password Set upon initial login

Platform Admin Email Administrator@company.com

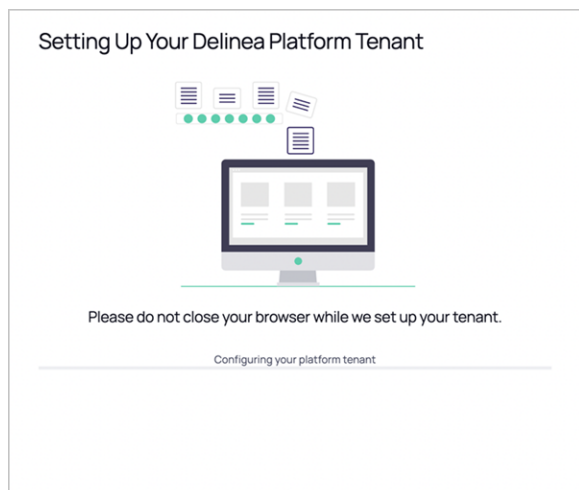
Connect Platform to Secret Server

Secret Server URL thetest.secretservercloud.com

Back Cancel Create Tenant

The platform begins provisioning a new tenant that is integrated with your Secret Server Cloud instance. A message is displayed asking you not to close your browser during setup, which is typically completed in 20 seconds or less.

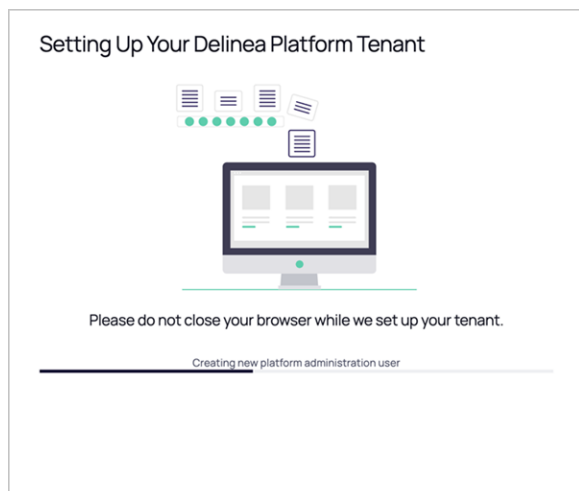
Adding Privileged Remote Access to Secret Server On Premises



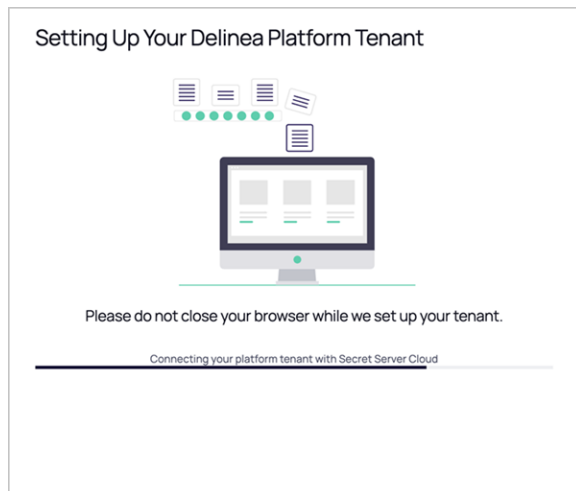
In the setup process, the platform performs the following actions:

- Configure and provision a new platform tenant
- Integrate your Secret Server Cloud tenant with your new platform tenant
- Create the new platform administrator account
- Send email to you with relevant information about your platform tenant

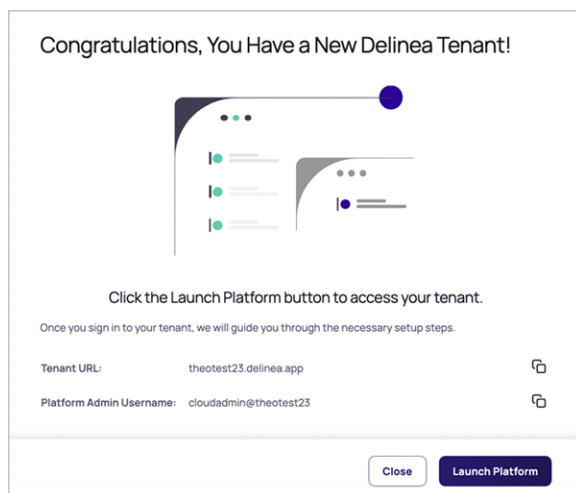
The setup message provides updates about the processes it is working on, as shown in the screen shots below:




Adding Privileged Remote Access to Secret Server On Premises



When setup is complete, a window appears with a success message.



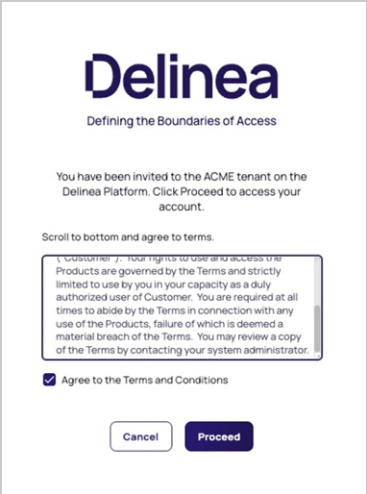
7. Copy your platform tenant URL and bookmark it (if desired), then click **Launch Platform**.

 **Note:** If the setup process takes longer than 60 seconds, a notification appears saying the setup is taking longer than expected. If you do not want to wait longer, you can safely leave the setup process, as long as you do not close the browser. Setup completes automatically, without further user input. You will receive an email notifying you when the process is finished.

Logging in and Getting Started

After you click **Launch Platform**, the login screen of your new Delinea Platform tenant is displayed.

Adding Privileged Remote Access to Secret Server On Premises

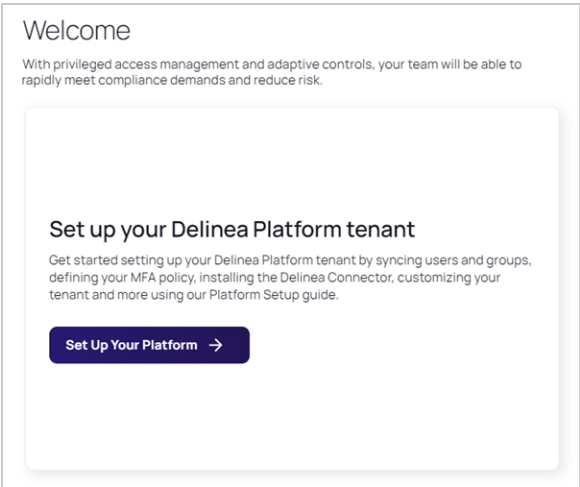


1. Click **Proceed**.
2. Update your password and click **Save**.

The image shows the "Set Password" form. It has a title "Set Password". Under "Password type", there are two radio buttons: "Manual" and "Generated", with "Generated" selected. To the right of the radio buttons is a "Copy Password" icon. Below this is a "Password *" field with a masked password "*****" and an eye icon to toggle visibility. At the bottom right is a "Save" button.

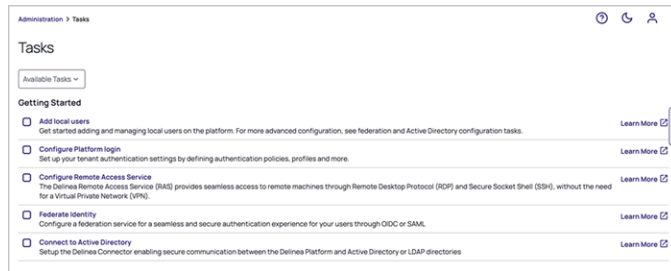
You are now logged in to your new Delinea Platform tenant. The platform Welcome screen opens.

3. On the Welcome screen, click **Set Up Your Platform**.



The **Tasks** page opens, displaying a list of optional tasks you can take to get started using the Delinea Platform.

Adding Privileged Remote Access to Secret Server On Premises



Use the **Learn More** link to the right of each task to learn how to accomplish the task.

To keep track of the tasks you've completed, you can check the box beside each task you complete.

Using Manual Integration

For Secret Server users to use secrets from the Delinea Platform, their Secret Server and platform accounts must share the identical login username. This is true for any administrative accounts used for setting up the Delinea Platform and Secret Server.



Note: Delinea Platform users working with a Secret Server cloud deployment (and URL) will not see Remote Access in the top-level left navigation. The PRA engine is automatically enabled to launch remote access for secrets that are based on appropriate templates.

New customers who sign up for a platform trial are assigned full administrator privileges within both the Delinea Platform and the integrated Secret Server Cloud.

When a new Delinea Platform user account is created and that user first logs in to the platform, the platform checks for an existing corresponding account (by username, domain, and UPN) in Secret Server. If a corresponding account already exists in Secret Server, the platform account is linked to the Secret Server account automatically. If there is no corresponding account in Secret Server, Secret Server automatically creates one and links it to the platform account. The two accounts appear to the user as a single account.


Retrieve the Platform Integration Credentials

1. Log in to the Delinea Platform with an administrative account.
2. Click **Settings** from the left navigation, then select **Authentication Profiles**.
3. Click the **Secret Server Connection** tab.

Adding Privileged Remote Access to Secret Server On Premises

The screenshot shows the 'Secret Server Connection' configuration page in the Delinea Platform. The page has a header with 'Administration >' and a search bar. Below the header, there are tabs for 'Authentication profiles', 'Configuration', 'Secret Server Connection' (selected), 'Security questions', and 'Security devices'. The main content area contains instructions: 'Use the client ID and client secret generated here to connect your Delinea Platform tenant to your Secret Server tenant. Navigate to the Platform Integration page in your Secret Server settings, and enter these values.' There are two buttons: 'Regenerate' and 'Test Connection'. Below this, there are four rows of configuration fields: 'Login URL' with value 'https://purpletrack-dev.secureplatform.io/identity/', 'Client ID' with value '8b663619-9fac-4c80-a2f0-ef30a8782fe1' and a copy icon, 'Client secret' with a masked value '*****', and 'Secret Server URL' with value 'https://purpletrack.devsecretservercloud.com' and an 'Edit' link. At the bottom, there is a 'Connection Status' field with a green 'CONNECTED' indicator.

4. Copy the **Client ID** and **Client Secret** and save them for use in the next section.
5. In the Secret Server URL field, add your Secret Server URL. For example, `https://<tenant>.secretservercloud.com`.
6. Click **Save**.

 **Note:** If you need to regenerate the credentials (Client ID and Client Secret), please contact Delinea [technical support](#).

To test the connection, click **Test Connection**. The connection status messages depend on your configuration, but could include *Connection was successful*, *Integration was not configured*, *Integration URLs do not match*, or *Did not receive an integration response*.

Enable Platform Integration in Secret Server

1. Log in to Secret Server with an administrative account.
2. Select **Administration > Tools & Integrations**.
3. Under **Tools & Integrations**, click **Platform Integration**.

[Admin >](#)



Platform Integration

[Configuration](#) [Groups](#) [Synchronization logs](#) [Audit](#)

Platform integration configuration

Configure platform integration settings here.

[Learn more](#)

Enable platform integration	Yes
<p> MFA settings for users authenticating via the Platform will be managed by the Platform. Secret Server Login MFA settings will not be honored.</p>	
Reply URL	<input type="text"/>
Login URL	<input type="text"/>
Client ID	<input type="text"/>
Client Secret	***** 
Profile name	secretserver
Logout URL	<input type="text"/>
Enable audit integration	Yes
Forward inventory data to Delinea Platform	Yes
Synchronization Interval	0 Days 1 Hours
Enable Platform On Login Page	Yes
Force Platform Only Login	No
Platform tenant's Id	<input type="text"/>
Vault Id	<input type="text"/>
Use platform settings	No

4. Click the **Configuration** tab.

5. Fill in the fields as follows:

- **Reply URL:** Pre-filled
- **Login URL:** The login URL displayed on the platform under **Settings > Secret Server Connection**; for example, `https://<hostname>.delinea.app/identity`.
- **Client ID:** The Client ID you copied in the previous steps
- **Client Secret:** The Client Secret you copied in the previous steps
- **Profile Name:** Pre-filled
- **Logout URL:** The logout URL endpoint for the platform; for example, `https://<hostname>.delinea.app/identity/api/Security/Logout`
- **Enable audit integration:** Yes. In future releases, this setting will probably not be optional.

- **Forward inventory data to Delinea Platform:** Yes. In future releases, this setting will probably not be optional.
- **Synchronization Interval:** Sets the interval for the Synchronize Platform function
- **Enable Platform on login page:** If Yes, the platform log in option appears on the Secret Server log in page. If No, the platform log in option is still accessible but not on the Secret Server log in page.
- **Force Platform Only Login:** Redirects to platform login
- **Platform Tenant's ID:** The platform tenant's unique identifier (read only)
- **Vault ID:** The identifier for the Secret Server instance (read only)
- **Use Platform settings:** Yes enables Unified Mode which consolidates role, user, and group management in the platform. After the systems are in sync, this is the last step of the Secret Server migration to platform. Once enabled, integral areas of the product are consolidated and this option cannot be disabled.

6. Select the **Enabled** checkbox.

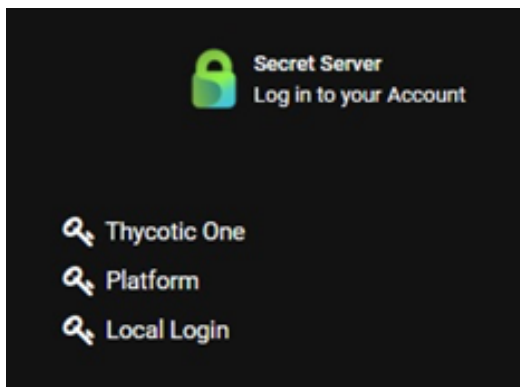
7. Click **Save**.

Verify the Integration in the Platform

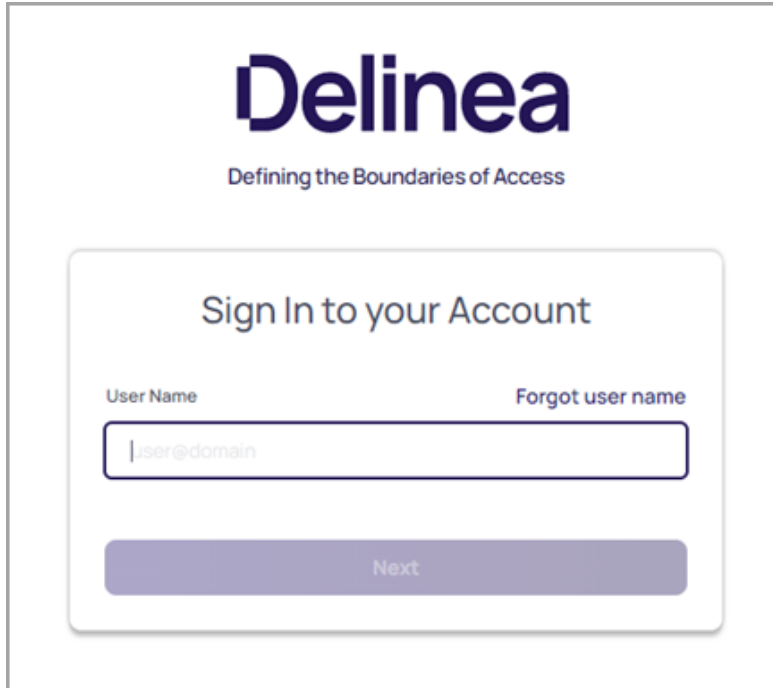
1. Log in to the Delinea Platform. If you're already logged in, log out, then log back in.
2. From the left navigation menu, click **Secret Server**, then select **All secrets** from the secondary menu.
3. The **All Secrets** page displays all of your secrets from Secret Server, now shared with the platform.

Verify the Integration in Secret Server

1. Sign out of Secret Server Cloud and return to the Secret Server login page.
2. When prompted for an identity provider, select **Platform**.



3. The Delinea Platform authentication screen displays.

The image shows a screenshot of the Delinea login interface. At the top, the Delinea logo is displayed in a large, bold, dark blue font, with the tagline "Defining the Boundaries of Access" in a smaller, lighter blue font below it. The main heading "Sign In to your Account" is centered in a dark blue font. Below this, there are two labels: "User Name" on the left and "Forgot user name" on the right. A text input field is positioned below these labels, containing the placeholder text "user@domain". At the bottom of the form, there is a wide, light blue button with the text "Next" centered on it.

4. Sign in with the credentials for the newly-created Delinea Platform account that maps to your Secret Server account.
5. If you can log in successfully, your integration between Secret Server Cloud and the Delinea Platform is complete.
6. Refresh the Delinea Platform page. The Secrets tab appears in the left navigation, and the browser launcher appears in Secret Server.

Because **cloudadmin** is not your Secret Server administrator account, while you are logged in as **cloudadmin** you will not be able to see your existing secrets in Secret Server or use your existing Secret Server administrator permissions. ***This is expected behavior and it does not indicate a failed integration.*** Do not change the **cloudadmin** username to match an existing Secret Server username, because that will break the synchronization between the Delinea Platform and Secret Server.

Link Platform and Secret Server Groups

When a platform user with administrator permissions in both platform and Secret Server identifies an existing platform group they want to link to a Secret Server group, the administrator provides Secret Server with the name of the platform group to be linked. Secret Server then retrieves the critical information about the platform group and uses it to automatically generate a new Secret Server group that is based on, linked to, and named for the original platform group.

These linked, automatically generated Secret Server groups are identified in Secret Server as ***Enabled Platform Groups***. For Enabled Platform Groups, Secret Server manages the Secret Server permissions, and platform manages the platform permissions. Platform also manages the group memberships, so all members of Enabled Platform Groups are platform accounts.

Adding Privileged Remote Access to Secret Server On Premises

Platform groups that can be linked to Secret Server groups this way include local as well as non-local platform groups, such as groups from external AD directories.

An Enabled Platform Group can coexist in Secret Server with a Secret Server-only group by the same name. The two groups remain distinct, and only one is identified as an Enabled Platform Group.

The group linking process moves in one direction: from the platform to Secret Server. So although you can link an existing platform group to a new Enabled Platform Group in Secret Server, you cannot link an existing Secret Server group to a platform group.

In this example, we will use *Platform Test Group* as the group name.

1. Click **Settings** from the left navigation, then select **Administration** below Secret Server.
2. On the Secrets Administration page, click **Platform Integration**.
3. Click the **Groups** tab.
4. Next to Enabled Platform Groups, click **Edit**.
5. In the **Select Groups** box, enter the name of a platform group that you want to sync to a new Secret Server group. In this example, *Platform Test Group* is the group name. Secret Server then queries the platform identity service and when it finds the group named Platform Test Group, the group's name is displayed beneath the Search field with a check box next to it.
6. Select the box next to **Platform Test Group**.
7. Click **Save**.

After the platform and Secret Server groups are linked, you can find the new Secret Server group named Platform Test Group from anywhere in Secret Server where groups are referenced. When you click to open **Platform Test Group**, the group page opens with a banner at the top stating, *The members of this group are managed by Platform*.

Synchronize Platform and Secret Server Groups

After the groups are linked, they are synchronized automatically at set intervals. The first time you link a platform group to a Secret Server group, the periodic synch might not happen immediately, so you might not see the platform accounts in the Secret Server group right away. To force the groups to synch:

1. Click **Settings** from the left navigation, then select **Administration** below Secret Server.
2. On the Secrets Administration page, click **Platform Integration**.
3. Click the **Groups** tab.
4. Click **Sync Now**.

The group synchronization process moves in one direction: from the platform to Secret Server. Existing platform groups synch to their linked Enabled Platform Groups in Secret Server, but existing Secret Server groups do not synch to platform groups.

Connecting to Secret Server On Premise

The integration of Secret Server On Premise (SSOP) with the Delinea Platform is limited to the [Remote Access](#) use case only. To use this integration, you must launch a Remote Access session from a vaulted secret stored in Secret

Adding Privileged Remote Access to Secret Server On Premises


Server On Premise. No secret server capabilities, such as lifecycle management, can be managed from the platform interface at this time.

Accessing the Delinea Platform

Current Secret Server On Premise customers can access the Delinea Platform and Privileged Remote Access by contacting a [Delinea sales representative](#) directly to request the Delinea Platform **without** the attached Secret Server Cloud.

After signing up for a trial, users will get a welcome email with the subject line, **Welcome to your Secret Server Cloud Trial on the Delinea Platform**. Follow the steps outlined in the welcome email to provision your platform tenant

Prerequisites

- Secret Server On Premise version 11.7.000015 or newer.
- An administrator account on both SSOP and on the Delinea Platform.
 -  **Note:** The Delinea Platform and SSOP accounts must share the same login username, and the user must be logged in with this username in both the platform and SSOP when following the steps below. This is true for any administrator accounts used for setting up the Delinea Platform and SSOP.
- Ensure that the network prerequisites are fulfilled to enable the integration between SSOP and the Privileged Remote Access feature on the platform.

Integration Steps

1. Install a Privileged Remote Access engine.
2. Add a new Secret Server On Premise connection to the platform.
3. Update the platform integration settings on Secret Server On Premise.
4. Update your Secret Server On Premise connection with the PRA site.
5. Verify the overall integration.

Install a Privileged Remote Access Engine

Deploy a Privileged Remote Access (PRA) Engine and ensure that the PRA Engine has access to your SSOP instance.

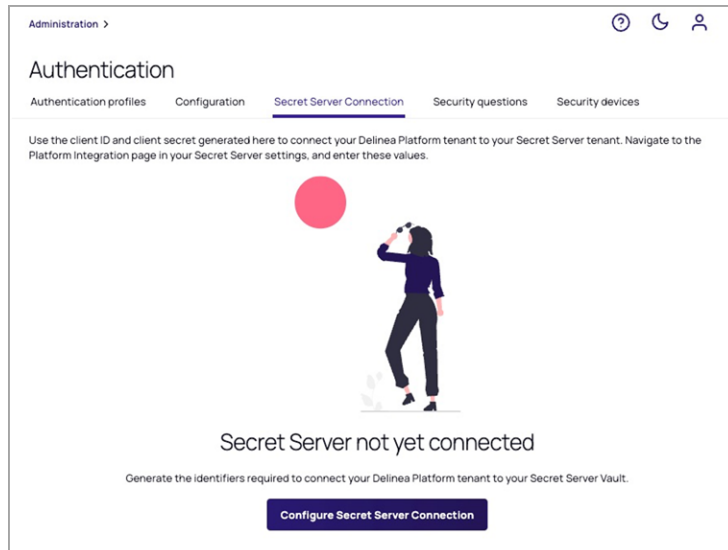
1. Log in to the platform.
2. Click **Settings** from the left navigation, then select **Remote Access**.
3. Follow the steps in [Privileged Remote Access](#) on installing a PRA Engine.

Add a New Secret Server Connection

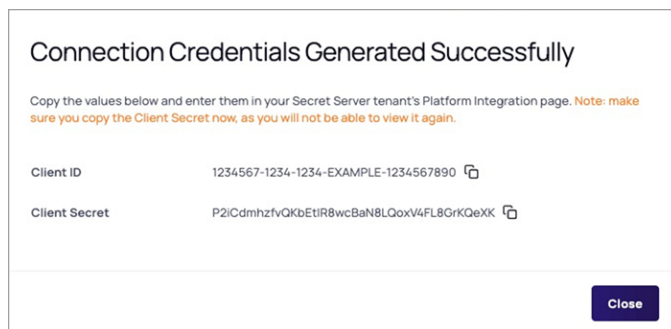
1. Log in to the platform.
2. Click **Settings** from the left navigation, then select **Authentication profiles**.

Adding Privileged Remote Access to Secret Server On Premises

3. Select the **Secret Server Connection** tab.
4. Click **Configure Secret Server Connection** to generate the required connection credentials.



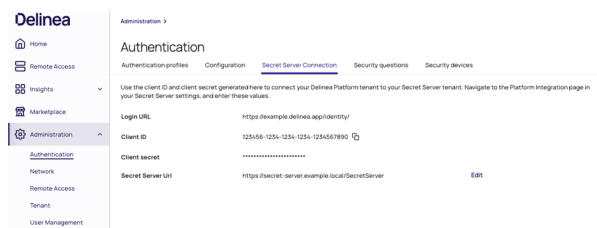
The platform generates a Client ID and Client Secret.



5. Make note of the Client ID and Client Secret values. You will need them later.

 **Note:** If you need to regenerate the credentials (Client ID and Client Secret), contact Delinea [technical support](#).

6. Update the Secret Server URL field, using the format `https://<hostname or IP address>/SecretServer`. For example, `https://secret-server.example.local/SecretServer`.



Update the Platform Integration Settings On Secret Server

1. Log in to your Secret Server On Premise instance.
2. Select **Administration > Platform Integration**.
3. Click **Edit**.
4. Update the following settings:
 - a. **Login URL**: the platform login URL that you copied from the earlier step
 - b. **Client ID**: the identifier assigned part of the OIDC connection
 - c. **Client Secret**: a secret used by Secret Server to authenticate with the platform

The screenshot shows the 'Platform Integration' configuration page. It has tabs for 'Configuration', 'Groups', 'Logs', and 'Audit'. The 'Configuration' tab is active. The page title is 'Platform Integration Configuration' with a subtitle 'Configure platform integration settings here.' and an 'Edit' button. Below this is a 'Learn More' link. The main configuration area includes: 'Enable Platform Integration' set to 'Yes' with a note about MFA settings; 'Reply URL' set to 'https://secret-server.example.local/SecretServer/signin-oidc'; 'Login URL' set to 'https://example.delinea.app/identity/'; 'Client ID' set to 'ddbba8a5-ca9e-4125-8a8b-ac954295c4e'; 'Client Secret' masked with dots and an eye icon; and 'Profile Name' set to 'secretserver'.

Update Your Secret Server Connection with the PRA Site

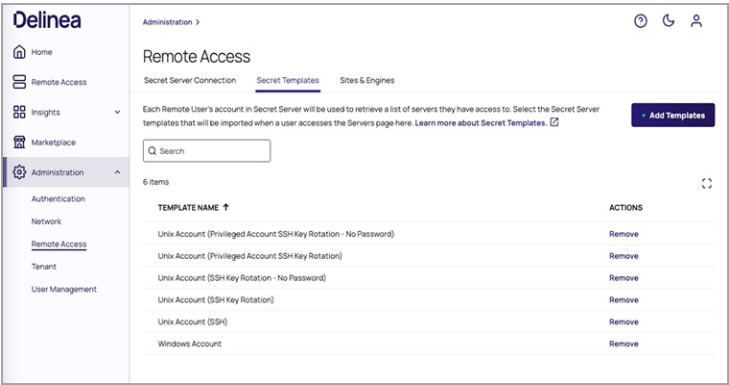
After the PRA engine is successfully installed, perform these steps:

1. Navigate to **Administration > Remote Access > Secret Server Connection**.
2. Click **Edit**.
3. Update the **Site** field with the PRA site that contains the engine you just created.

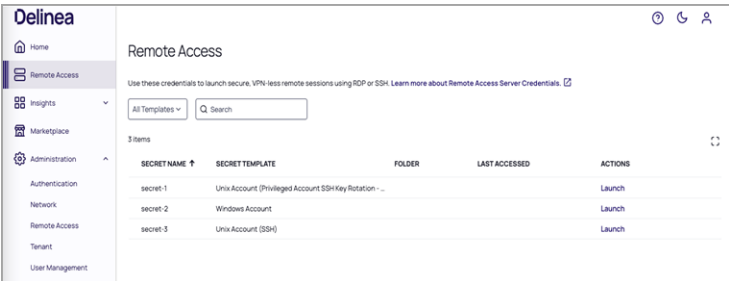
The screenshot shows the 'Secret Server Connection' page under 'Remote Access'. It has tabs for 'Secret Server Connection', 'Secret Templates', and 'Sites & Engines'. The 'Secret Server Connection' tab is active. The page title is 'Secret Server Connection' with a subtitle 'Configure the Secret Server vault connection here.' and an 'Edit' button. Below this is a 'Learn more about connecting to Secret Server.' link. The main configuration area includes: 'Connection Status' showing 'CONNECTED' in a green box; 'Location' set to 'On-Premises'; 'Secret Server URL' set to 'https://secret-server.example.local/SecretServer'; and 'Site' set to 'Ireland'.

Verify the Overall Integration

1. Log in to the Delinea Platform.
2. Select **Administration > Remote Access > Secret Templates**. A default set of Secret Server templates displays. You can add other templates as desired by clicking **Add Templates**.



3. Select **Remote Access** from the left navigation menu. Typically, secrets created by or shared with the logged-in user are listed.



You can now launch Remote Access sessions from the secrets that support PRA by clicking the **Launch** link under the **Actions** column.

Setting Up Resilient Secrets


Secret Server offers Resilient Secrets for organizations to protect and recover their IT infrastructure and data as part of an overall disaster recovery strategy. ([Learn more](#)).



Important: The Resilient Secrets functionality does not fully replace a business continuity strategy and should not be used as a failover feature.

Prerequisites

- A Delinea Platform instance integrated with Secret Server.
 - Delinea Platform customers after November 2023 already have Secret Server Cloud integrated.
 - Legacy customers of Secret Server Cloud who migrate to the Delinea Platform must integrate the two products.
 - Secret Server on-premises customers who purchase the Delinea Platform to use PRA can perform a manual integration.
- An additional Secret Server cloud or on-premises instance that will act as the replica. This instance must not be connected to any other Delinea Platform.

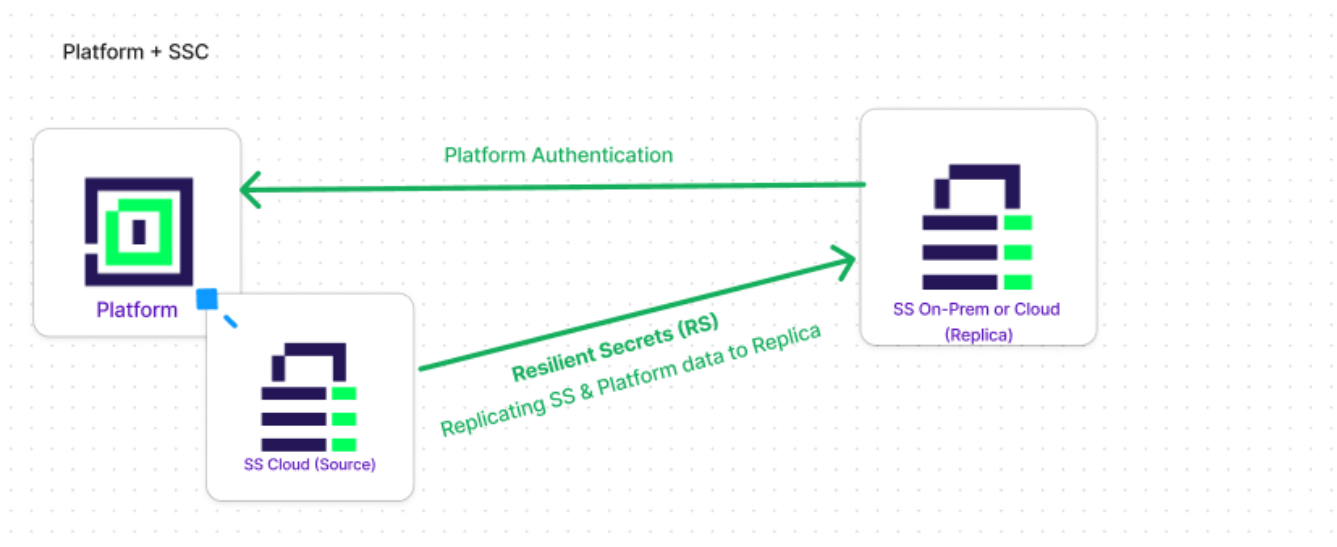
 **Important:** Customers have the option to buy more than one instance of Secret Server, if they want to have multiple replicas.

 **Note:** The Secret Server requirements for replica instances are the same as for the source instance.

How Do Resilient Secrets Work?

The Resilient Secrets feature copies information from the source Secret Server instance to the replica. Information on the replica Secret Server will be overwritten by the source for anything copied.


The configurations for the Cloud and On-Premises replicas are the same. There is nothing you would need to do differently, configuration wise, when setting up a Cloud replica as opposed to On-Premises and vice-versa. The following diagram represents the flow of data from the source instance to the replica in both the Delinea Platform and Secret Server respectively:



- The Delinea Platform is connected to Secret Server via an encrypted connection.
- Secret Server (Source) is connected to a replica (either Secret Server Cloud or Secret Server On-Premises) via an encrypted connection.
- The replica pulls the data package from the Source.

Adding Privileged Remote Access to Secret Server On Premises


- When the Delinea Platform is available, users can log in to the replica with their Delinea Platform credentials.
- When the Delinea Platform is not available, users can log in to the replica via SAML or via local accounts

 **Note:** Only one Delinea Platform and Secret Server Cloud pair is supported.

Best Practices

- **Read-Only Mode:** Replicas should be in read-only mode during operation because there can only be one source of truth - the Source instance.
- **Cloud Replicas:** For a replica Secret Server Cloud, Delinea recommends setting it up in a different geographic region (if both replica and cloud instances are in the same region, an issue impacting that region could disrupt both).
- **On-Premises Replicas:** For the replica (Secret Server on-premises), Delinea recommends creating local accounts on that instance so that, in the event of a complete service outage, you will still be able to log in to the replica instance with your local account.

 **Important:** Do not set up directory sync on the replica instance. This can cause duplicate users to appear when syncing users with the Delinea Platform.

 **Note:** Do not enable User Sync under Directory Services on your replica instance while also having Resilient Secrets replicate Users from the same directory. This configuration can cause conflicts with replication and eventually may cause database deadlocks.


- **On-Premises Systems:** On-Premises systems involved in Disaster Recovery/Resilient Secrets a Source or Replica require a site connector using RabbitMQ

Delinea Platform with Secret Server Cloud and Replica Secret Server Cloud

Cloud replicas respect the user login settings of the Delinea Platform. All configurations are copied from the Delinea Platform to the replica Secret Server Cloud.


In the event of a service outage where the source Secret Server Cloud goes down, users will still be able to log in to the replica Secret Server Cloud tenant using their Delinea Platform credentials.

If you have an external user source (Entra ID, Okta, etc.) for Platform login, those log-ins will also work with the Cloud replica, as long as those sources are still online. If federation providers are down, you can log into Secret Server with your local accounts.

 **Note:** Local Accounts should be created ahead of time, before a Disaster Recovery event occurs.

Delinea Platform with Secret Server Cloud and Replica Secret Server On-Premises

On-premises replicas respect the user login settings of the Delinea Platform. All configurations are copied from the Delinea Platform to the On-Premises replica.

 **Note:** After logging in to the On-Premises replica with your Delinea Platform credentials, you will still be in the Secret Server On-Premises UI.

Typically, a user could log in to the on-premises replica from its login page using their Delinea Platform credentials, but to prepare for an outage, you must have alternative methods available.

Make sure the On-Prem replica has an outbound rule allowing traffic to the Cloud source over port 443 (HTTPS).

On-Premises Replica Authentication for Delinea Platform-Based Login

In the event of a service outage, the Delinea Platform login capability will not be available. To ensure access during an outage, you should prepare an alternative login method, such as configuring SAML for your IdP source (see [SAML and OIDC Federation](#)) which will allow users to log in with their Delinea Platform credentials. The IdP can be a self-hosted SAML provider (ADFS or other self-hosted option) and does not need to be the same IdP as used by the Delinea Platform.

On-Premises Replica Authentication for Federation-based Login

In the event of a service outage that interrupts federated credential providers (Entra ID, Okta etc.), users will still be able to log in as long as you have:

1. Configured both source and replica to accept those federation services.
2. Configured the on-premises replica to use SAML. If the user source is also down, you will only be able to log in with local accounts.



Important: In the event of a service outage, administrators who set up a local account for their on-premises replica will still be able to log in with that account. Any other local accounts you create will also be able to log in.

On-Premises Source With Cloud Replica (SSC or Platform)

- Make sure the on-premises source has an inbound rule allowing traffic from the Cloud replica over port 443 (HTTPS).
- Make sure you have a custom URL set.

Frequently Asked Questions

1. How does the Secret Server Primary Source connect to Delinea Platform?

The Primary Secret Server (Source) is connected to the Delinea Platform via an encrypted connection. On the Delinea Platform see (**Settings > Secret Server Connection**). At this time, only one connection from Delinea Platform to Secret Server is possible.

2. How are Resilient Secrets licensed? Do you get just Resilient Secrets (Secret Server Cloud) or a new instance of the Delinea Platform + Secret Server Cloud?

Since Resilient Secrets is a functionality of Secret Server, every instance of Secret Server needs to be licensed. You can only have one instance of the Delinea Platform and Secret Server, acting as the Source, but you may choose to purchase multiple Replica instances.

3. How does a Secret Server Cloud Replica need to be configured with the Primary Delinea Platform + Secret Server Cloud Source?

There is no special configuration for Cloud or On-Premises replicas to connect to the Delinea Platform. This is done on the Primary (Source) Secret Server. Please refer to [Setting Up Resilient Secrets](#) for more information.

4. Will Resilient Secrets work if you have 2 instances of the Delinea Platform - each connected to their OWN Secret Server Cloud - EXAMPLE - 2 instances of the Delinea Platform and 2 Instances of Secret Server Cloud.

No, Secret Server Cloud only supports one Delinea Platform instance at a time. (The Source)

5. How does Platform in Secret Server Cloud Unified roles and permissions work with Resilient Secrets?

In unified mode your primary instance of Secret Server Cloud (the source) pulls role and permission assignments from platform. This information is then replicated/copied over to the replica Secret Server.

6. How do you configure Resilient Secrets to ensure you have access to Secrets when the Delinea Platform Is NOT Available?

There are two ways you can log in to your Replica instance if the Delinea Platform is not available:

- a. Configure SAML: Configure SAML with your IdP (Identity Providers)
- b. Logging in with local accounts - In the event that everything fails, you will need to have created “break glass” local accounts on the Replica Secret Server. As mentioned in the Best Practices section earlier, Delinea recommends creating these local accounts as soon as you provision the Replica instance.

7. How do you configure Resilient Secrets to ensure you have access to Secrets when Entra ID (Azure AD) is not available?

Configure SAML with your IdP and/or create local accounts on the Replica instance so you can log in when no directory services are available.



Note: If you create local accounts on the source, they will be copied to the replica.

8. How do I download and Install Resilient Secrets as a Delinea Platform customer?

Resilient Secrets is built upon Secret Server. To have Resilient Secrets on-premises you will need to install Secret Server On-Premises (see downloading Secret Server). If you want Resilient Secrets in the Cloud, you will need to have a second instance of Secret Server Cloud.

Please contact Delinea Sales or Support for purchase questions.

9. I'm in the process of transitioning from Secret Server Cloud to the Delinea Platform. I have a Replica Instance (on-premises or cloud). Upon standing up the Delinea Platform, tenant secrets are no longer synced.

- Look for errors in the Resilient Secrets replication logs (Disaster Recovery Log tab on the Replica).
- If secrets are skipped, some vital data may be missing.
- Run a manual replication by going back a few years or using a date like 1/1/2000 to perform a full sync. If this does not resolve the issue and you cannot determine the errors from the logs, please reach out to support and open a case/work item.

Resilient Secrets Login Options

Below are the login options available to users depending on service availability and internet connectivity:

Service Availability	Delinea Platform Cloud	Secret Server Cloud	Secret Server On-Premises	Resilient Secrets Cloud	Resilient Secrets On-Premises
Delinea Platform Available	Login via Delinea Platform Credentials	Login via Delinea Platform Credentials	Login via Delinea Platform Credentials	Login via Delinea Platform Credentials	Login via Delinea Platform Credentials
Delinea Platform Not Available	No Login Available	Login via SAML or Secret Server Local Accounts	Login via SAML or Secret Server Local Accounts	Login via SAML or Secret Server Local Accounts	Login via SAML or Secret Server Local Accounts
Delinea Platform Available, but the Identity Provider is Not Available	Delinea Platform Local Account Login	Delinea Platform Local Account Login	Delinea Platform Local Account Login	Delinea Platform Local Account Login	Delinea Platform Local Account Login
Delinea Platform Not Available and the Identity Provide is Not Available	No Login Available	Secret Server Local Account Login	Secret Server Local Account Login	Secret Server Local Account Login	Secret Server Local Account Login
Standalone Secret Server (Without the Delinea Platform)	Not Applicable	Active Directory/ Identity Provider Login or Secret Server Local Account Login	Active Directory/ Identity Provider Login or Secret Server Local Account Login	Active Directory/ Identity Provider Login or Secret Server Local Account Login	Active Directory/ Identity Provider Login or Secret Server Local Account Login
No Internet Connectivity	No Login Available	No Login Available	Secret Server Local Account Login or Active Directory/ Identity Provider, if available on intranet	No Login Available	Secret Server Local Account Login or Active Directory/ Identity Provider, if available on intranet

Server Suite on Delinea Platform

This guide is for Server Suite customers who wish to use Server Suite along with Delinea Platform. It describes:

- Using MFA for Server Suite
- Direct Audit Integration with Platform

Release Notes

- [Change Log](#)
- [Spring \(Q2\) 2025 Release](#)
- [Winter \(Q1\) 2025 Release](#)
- [Fall \(Q4\) 2024 Release](#)
- [Summer \(Q3\) 2024 Release](#)
- [Spring \(Q2\) 2024 Release](#)
- [Winter \(Q1\) 2024 Release](#)
- "Fall (Q4) 2023 Release" on page 825
- "Summer (Q3) 2023 Release" on page 827
- [Spring \(Q2\) 2023 Release](#)
- [Winter \(Q1\) 2023 Release](#)

Please Wait...

Spring (Q2) 2025 Release

Secret Server on Platform

Azure Key Vault (AKV) Integration (in GA): Streamline secret and Non-Human Identity management with native integration to Azure Key Vault. This enhancement enables centralized secret updates, supports frequent rotation, and enforces governance with fine-grained roles, permissions, and full audit logging. Learn more about this capability [here](#).

Continuous Identity Discovery (CID)

Active Directory (AD) Support for CID (in GA): CID now supports Active Directory environments. Key features include:

- Discovery of privileged users (including admin, shadow, and other elevated accounts) through ACL-based permission analysis

- Enhanced AD visibility with the ability to view and filter directory data for easier investigation and management
- Learn more about this capability [here](#).

Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)

Google Cloud Platform (GCP) support for ITP (in GA): You can now integrate GCP with the Delinea Platform (ITP) to extend identity-centric security across your Google environment. This integration enhances access management and helps secure privileged identities by providing visibility into the following:

- GCP Role Refactor - Identify unused permissions within GCP roles to help you move toward a least privilege model.
- GCP Shadow Admin Check - detect shadow admins, non admin users with the ability to escalate their access to administrative
- Identify Non-Vaulted Accounts - Gain visibility into privileged, admin, and shadow accounts that aren't properly vaulted.
- Non-Rotated Access Keys - Identify and address non-rotated keys to ensure your security practices align with best practices for key management.
- Visibility - Identify and query users' access in workspace admin directory and GCP to explore their access per project
- Learn more about this capability [here](#).

Account MFA Factors (in GA): Organizations often struggle with limited visibility into the Multi-Factor Authentication (MFA) factors enabled across their cloud environments. With the general availability of Account MFA Factors, customers can now gain insights into the MFA methods enabled and their security level, quickly identifying high-risk users with weak authentication factors. Learn more about this update [here](#).

Analytics

Analytics Now (in Public Preview): Analytics provides deeper visibility into user behavior and risk, helping organizations strengthen their security posture. Key features include the following:

- Real-time risk scoring based on behavior and authentication threats
- Detection of anomalies and behavioral changes
- Near real-time threat investigation and response
- Customizable risk parameters to reduce false alerts and align with your policies
- Learn more about this new service [here](#).

Identity Lifecycle Management (ILM)

Identity Lifecycle Management (ILM) (in Private Preview): ILM streamlines the entire user identity lifecycle—from onboarding to offboarding—by dynamically adjusting access as roles evolve. Key features include the following:

- Automated Joiner-Mover-Leaver Processes: Seamlessly create and manage identities, provision access at onboarding, and adjust or revoke access as users change roles or exit.

- **Security & Compliance:** Built on the cloud-native Delinea Platform, ILM leverages real-time identity and access context to detect risk, enforce policies, and manage access automatically.
- **Intuitive Workflow Design:** Easily configure lifecycle workflows with a no-code, drag-and-drop interface—no custom coding required.
- Learn more about this new service [here](#).

Privileged Remote Access (PRA)

PRA Workloads (in GA): PRA capabilities are now available through a unified deployment on the Delinea Platform Engine, with centralized management via the Engine Management interface. This is supported on both Windows and Linux. As part of this change, PRA no longer supports the creation of new Sites or the installation of new Engines for standalone PRA engine. Tenants requiring new Sites or Engines must now use Platform Sites and deploy Platform Engines with PRA capabilities. Note that previously deployed PRA sites and standalone engines will continue to function normally but will not be updated to support new functionality on the future roadmap. Learn more about this new capability [here](#).

Connection Manager (CM)

Connection Manager 2.6 Release

- **External Browser MFA for Secrets:** This update extends external browser-based MFA to protect access to secrets, adding a new layer of security through the Delinea Platform. Previously, this MFA method only supported platform login.
- **Fullscreen Display Support for macOS:** Users on macOS can now enjoy a more seamless and native full screen experience in CM, enhancing overall usability.
- **New SSH Terminal for macOS:** A redesigned SSH terminal delivers improved performance, user experience, and convenience for macOS users.
- More updates and enhancements are detailed in these [release notes](#).

Connection Manager 2.6.1 Release

- This release addressed a couple bug fixes and their related improvements. See [release notes](#) for additional details.

Inventory

Permissions on Collections (in Public Preview): You can now assign granular permissions to computer collections, allowing precise control over which computers end users can view and interact with. This new capability currently supports computer collections, with plans to extend to additional asset types in the future. This update also introduces a new permission specifically for launching access with Privileged Remote Access (PRA), along with UX enhancements to streamline the setup and management of these permissions. Learn more about this new capability [here](#).

Identity and Federation

Non-Interactive Service User Option (in GA): To help customers enforce the intended use of service users—automation, not interactive access—we've introduced a new non-interactive option in identity policies. When enabled, this setting prevents service users from logging in through the UI, reducing the risk of misuse and

strengthening overall security. Interactive login remains available when needed, but customers now have full control over how service users can access the platform. Learn more about this update [here](#).

Engine Management

Enhanced Web Proxy Support for Deployments (in GA): This update addresses issues where restrictive web proxy settings block configuration file downloads, leading to deployment failures. We've introduced improved proxy handling across Engine binary download, configuration file retrieval and engine service communication. Learn more about these updates [here](#).

Marketplace and Integrations

View Configured Integrations: Added the ability to view all configured integrations, providing greater transparency and easier management. Learn more about this update [here](#).

Download Center UX Improvements: Improved usability in the Download Center for a more streamlined and intuitive experience. Learn more about the Download Center [here](#).

New and Updated Integrations:

- CrowdStrike Falcon Fusion SOAR Integration GA
- Addition of GitGuardian Scout Integrations for Delinea Platform GA
- Keyfactor Control Integration GA
- Avantra AIOPs for SAP for Delinea Platform GA
- RabbitMQ Helper 12.1.0
- Oracle JDBC Proxy Driver to support Delinea Platform
- Rapid7 InsightVM with Delinea Platform
- Integration with ConnectWise Screen Connect V4.0 to support Delinea Platform
- External Secrets K8 Integration
- Utimaco support for u.trust General Purpose HSM Se-Series

Other Updates

United Arab Emirates (UAE) databoundary availability: Customers with data residency requirements in the UAE and neighboring regions can now deploy the Delinea Platform and Secret Server Cloud within the UAE. This new regional deployment offers reduced latency and enhanced performance for customers in this region. Learn more about regional availability [here](#).

Delinea Platform Mobile App: Vaulting capabilities are now available in the Delinea Platform Mobile app, expanding on the existing mobile features to deliver a more complete, end-to-end experience for users managing the platform on the go. This update empowers users with greater control and flexibility, even when away from their workstation.

- Create and edit Secrets directly from the mobile app
- Complete security workflows on the move
- Access vaulted credentials securely from your mobile device

Improved Grid Filter Persistence for Seamless Task Switching: We've made it easier to pick up where you left off. Full-page grids can now remember your filter settings between sessions, reducing time spent reapplying filters when returning to previous tasks. Turn on the "Remember filter values" option under User Preferences in Platform to start using this feature.

Secret Icons for a More Intuitive Experience: Icons can now be associated with Secret Templates to make it easier for users to visually identify and interact with different types of secrets. Learn more about this update [here](#).

Performance and Resiliency Enhancements for Policy Propagation: Several improvements added to ensure smoother and more reliable policy propagation for Privilege Control for servers, especially in environments with a high volume of policies. Key updates include the following:

- Enhanced resiliency for Command Relay under load
- Optimizations to messaging queue handling for better throughput and stability
- Improved processing efficiency for collections, reducing latency and improving scalability

Winter (Q1) 2025 Release

Secret Server (SS) on Platform

- **Platform Integration Center** (in private preview): Designed to provide a path for existing Secret Server Cloud tenants to fully integrate with the platform, from standalone tenants through to fully unified. Learn more about this update [here](#).
- **Event-Driven User and Mapping Updates:** Secret Server now supports near-real time updates for user mapping changes through event-driven processing.
- **Entra ID Discovery Enhancements:**
 - **Account Type Filtering:** Added the ability to filter Entra ID account types during Discovery, including options to exclude External Accounts and Synchronized On-Premises AD Accounts.
 - **Heartbeat and MFA Enrollment:** Heartbeat checks now support accounts pending MFA enrollment, with improved error handling for reliability.
 - **Role Assignments via Groups:** Entra ID Discovery now identifies role members assigned through group memberships.
- **Improved Search Performance:**
 - Resolved performance issues during secret searches by optimizing internal logic to limit searches to user-accessible secrets.
 - Enhanced database handling by eliminating deadlocks and significantly improving performance.

Continuous Identity Discovery (CID)



Note: Continuous Identity Discovery was previously referred to in Delinea Platform as Continuous Identity Discovery.

- Continuous Identity Discovery (CID) (in GA) helps discover privileged cloud identities, including admins, shadow admins, and privileged non-human identities that are not vaulted in Secret Server and suggest vaulting

them in a click of a button. Learn more about this new service [here](#).

- **Continuous, Out-of-the-Box Discovery:** Discover privileged accounts, including shadow admins, admins, and both local and federated accounts, without the need for custom scripts.
- **Detect PAM Bypassing:** Identify users accessing cloud applications directly, bypassing the vault.

Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)

- **Workday integration** (in GA) - leverage Workday as a source of truth for better visibility and posture.
 - Gain a comprehensive view of your workforce with enriched identity-level information.
 - Use Workday as a trusted source-of-truth to discover partially off-boarded users and external accounts.
 - Enhance identity merging by leveraging diverse account properties like email and employee ID.

Learn more about this new integration [here](#).

- **Introducing Cases** (in GA): Incidents are being replaced with a new layer for security findings in ITP and PCCE, designed to reduce noise by grouping alerts based on predefined logic, such as attack patterns or entities. Cases are now the central location for customers to access actionable, security-relevant items. Learn more about this update [here](#).

Analytics

- **Introducing Analytics** (in Private Preview), enabling organizations to gain deeper insights into user behavior and risks while maintaining their security posture.
- **Know Your User Risk:** Monitor and identify your riskiest users with automatically calculated risk scores based on behavioral patterns and authentication threats, making it easy to spot anomalies.
- **Recognize Behavioral Change:** Detect deviations from normal activity, with baseline behavioral indicators so you can identify and respond to potential threats with efficiency and precision.
- **Proactively Protect Accounts:** Protect all accounts from attacks by recognizing when there is a potential threat in progress and investigate in near real-time before they get in and cause damage.
- **Customize Risk Parameters:** Adjust scoring weights and alert thresholds to align with your organization's specific needs. Customization is key to making security work for you by ensuring you set the rules to avoid false alerts and irrelevant workflows.

Learn more about this new service [here](#).

Privileged Remote Access (PRA)

- **PRA Workloads** (in Public Preview): Unified deployment of PRA capabilities on the Delinea Platform Engine and a centralized Engine Management interface. Available for both Windows and Linux. Learn more about this new capability [here](#).
- **Kerberos Support** (in GA): PRA users can now securely access target machines within Windows Domains that utilize Kerberos authentication.
 - **Enhanced Security:** Kerberos mitigates risks associated with NTLM, including Pass-the-Hash, DC Sync, NTLM-relay, and other attack techniques. Refer to Microsoft's NTLM deprecation announcement for more

details.

- **Seamless Integration:** For customers using both Kerberos and NTLM, the "fall back to NTLM if Kerberos fails" approach ensures uninterrupted access and flexibility. Learn more about this update [here](#).
- **New Disconnect Remote App Session:** A new Ctrl+Alt+Delete shortcut added to the Disconnect menu in PRA to prompt users to sign out from their session. Learn more about this update [here](#).

Connection Manager (CM)

- **Connection Manager 2.5.4 Release**
 - **Simplified Authentication Flow:** Users can now authenticate to Secret Server via an external browser without needing to click on a Secret Server page to launch Connection Manager.
 - **Preconfigured Vaults for Administrators:** Administrators can preconfigure multiple vaults, eliminating the need for users to create connections when opening Connection Manager for the first time.
 - **Additional Updates:** More updates and enhancements are detailed in these [release notes](#).

Privilege Control for Servers (PCS)

- **Run As Service Account or Domain Group.** This feature is part of the Granular Commands capability (in GA) allows applications to run as an Active Directory user or domain group, eliminating the need to log in as a specific user to complete tasks. Learn more about this new capability [here](#).
- **Multi-Factor Authentication (MFA) for Server Suite** (in GA). Server Suite customers can now integrate with the Delinea Platform as an MFA source. Learn more about this new capability [here](#).

Inventory

- **Collections** (now in GA): This new capability allows computers to be grouped by shared attributes for easier management. Policies can now be streamlined and applied to collections, minimizing manual effort. Additionally, collections automatically update as new computers meet the defined criteria, enhancing scalability and ensuring that asset management remains efficient as the environment grows. Learn more about this new capability [here](#).
- **Permissions on Collections** (in Private Preview): You can now assign detailed permissions to computer collections, controlling which computers an end user can view and interact with. This capability currently applies to computer collections, with more asset types to be added in the future. Learn more about this new capability [here](#).

Identity & Federation

- **Enhanced Security with Duo Integration** (now in GA): Customers can enable Duo MFA for an extra layer of security during login and authentication, strengthening their security posture while ensuring a seamless user experience. Learn more about this new integration [here](#).
- **Native Entra ID Integration** (in Private Preview): The Delinea Platform introduces a direct API integration with Microsoft Entra ID, offering seamless SSO login and MFA using Entra ID credentials. This integration enables direct usage of Entra ID groups without the need for local mapping or user claim mapping. It also provides a streamlined experience for browsing Entra ID groups and users within the platform, while supporting the pre-

assignment of users to roles and permissions prior to their first login. Learn more about this integration [here](#).

- **Federation Automated Group Mapping** (in Private Preview): This feature dynamically creates and assigns groups based on group claims received from the IdP during user authentication, eliminating the need for manual configuration. This enhancement saves time, reduces effort, and minimizes the risk of human error when group mapping at scale. Learn more about this feature [here](#).
- **Platform Service Account Creation Improvements**: We've enhanced the service user creation workflow, making it easier to set up non-interactive, programmatic access for API integrations and automation scripts. These improvements streamline the process, reducing setup time and complexity. Learn more about this update [here](#).
- **Integrated Windows Authentication (IWA) Host Certificate** (now in GA): In addition to the option to import your own certificate, you can now generate a self-signed certificate with a single click, making setup and management of IWA more efficient. Learn more about this update [here](#).

Engine Management

- **At a Glance view**:
 - Users can view the 'at a glance' summary of the site, including the Engine and its Workloads.
 - Easily check the status of Workloads with fewer clicks.
- **Auto update maintenance window**:
 - Users can choose site-level settings to automatically update their engines.
 - Schedule updates for specific times and days.

Learn more about these updates [here](#).

Marketplace & Integrations

- **Download Center** (now in GA): Now have ability to download up to 3 previous versions of the software packages. Learn more about this capability [here](#).
- **Marketplace Quick Filters** - ability to use Quick filters to filter top integrations. Learn more about this update [here](#).
- **New and Updated Integrations**:
 - Microsoft Defender for Identity Integration with Secret Server (in Private Preview). Learn more about this new integration [here](#).
 - ITP/PCCE: GCP Integration GA
 - MFA: Cisco Duo native in Platform GA
 - Splunk Cloud Integration via Webhooks
 - Direct Entra ID API Integration
 - Workday ITP/CID Integration GA
 - RabbitMQ Helper 12.0.0
 - Terraform SS Integration upgrade 2.0.10

Release Notes

- Jenkins Release 1.1.0/1.1.1
- SCIM on prem 4.7.0
- Secret Server SDK support
- Terraform 2.0.10
- ServiceNow Xanadu certification for all Delinea ServiceNow Integrations

Other Updates

- **Webhooks Security** (now in GA): Use webhook secret to verify the legitimacy of the webhook request and protect against man-in-the middle attacks. Learn more about this new feature [here](#).
- **Combined Discovery** (in Public Preview): You can now create and manage both Identity Threat Protection (ITP) and Secret Server (Vault) discovery sources. The two "Sources" pages have been combined under Discovery for a more streamlined experience. Learn more about this update [here](#).

Fall (Q4) 2024 Release

Secret Server (SS) on Platform

- **Entra ID Discovery Expansion:** The discovery capabilities now include the new Entra ID Discovery source and scanners, broadening visibility and access to Entra ID resources. Learn more about this update [here](#).
- **Entra ID Remote Password Enhancements:** A series of updates to improve handling of Entra ID accounts, specifically:
 - Processing heartbeats for Entra ID accounts requiring MFA
 - Processing heartbeats for Entra ID accounts with Conditional Access Policies that enforce MFA.
 - Learn more about this update [here](#).

Continuous Identity Discovery (CID)

- **Expanded Identity Coverage:** Improve your organization's identity security with enhanced discovery capabilities in Secret Server Cloud on the Delinea Platform. CID now covers cloud identities including privileged accounts, service accounts, admins, and shadow admins.
- **Automated Monitoring of Sensitive Accounts:** CID operates automatically and continuously, enabling seamless monitoring of sensitive accounts. Privileged credentials can be quickly vaulted in Secret Server as needed, ensuring secure storage and reducing the risk of unauthorized access.
- **Enhanced Discovery and Access Customization:** Easily discover privileged users, including those with stale credentials or lacking MFA. CID also enables quick customization of access, helping you keep user privileges current and aligned with security policies.
- Learn more about this new service [here](#).

Identity Threat Protection (ITP) and Privilege Control for Cloud Entitlements (PCCE)

Snowflake Integration:

- **Enhanced User Visibility:** Easily identify and manage user accounts without MFA and partially off-boarded accounts.
- **Privileged Account Discovery:** Detect privileged roles and accounts based on assigned permissions.
- **Comprehensive Health Checks:** Ensure your Snowflake environment's security and compliance with thorough health checks.
- **Attack Detection Rules:** New rules targeting password and MFA-based attacks on Snowflake.
- Learn more about this new integration [here](#).

Privileged Remote Access (PRA)

- **PRA Workloads** (*in private preview*): Unified deployment of PRA capabilities on the Delinea Platform Engine and a centralized Engine Management interface. Learn more about this new capability [here](#).
- **File Transfer Enhancements:** Prevent accidental data loss while transferring files between local and remote systems. Users can see when file transfers are active and they are notified if they try to close the remote connection.
- **Remote Applications:** Access published RDS desktop applications rather than entire systems, enforcing least privilege access and reducing the potential attack surface and associated security risk. Learn more about this new capability [here](#).

Connection Manager (CM)

Available in Connection Manager 2.5.3 Release:

- **RDP Connection Timeout over TCP:** Connection Manager now allows MacOS users to customize the RDP connection timeout over TCP. This is helpful for extending the timeout in scenarios involving proxy or MFA. Learn more about this update [here](#).
- **MacOS 15 Sequoia Support:** Supports the latest MacOS release.
- **Additional Updates:** More updates and enhancements are detailed in these [release notes](#).

Privilege Control for Servers (PCS)

- **Granular Commands Capability** (*in private preview*):
 - **Minimize Standing Privilege:** Define specific commands within PCS policies for Windows, Linux, and Unix, ensuring users can elevate only what they need.
 - **Enforce Least Privilege:** Limit elevated user actions to pre-approved commands, reducing security risks.
 - **Enhanced Security and Control:** Prevent unauthorized elevated actions with command-level restrictions.
 - Learn more about these new capabilities [here](#).
- **Targeting Machines in AD without Agents:**

- **Enhanced Policy Targeting:** Apply PCS policies to Active Directory (AD) machines without requiring an agent to be installed first.
- **Faster Onboarding:** The onboarding process has been streamlined to accelerate time-to-value.
- **Collections** (*in private preview*):
 - **Dynamic Asset Grouping:** Group computers by shared attributes for simplified management.
 - **Streamlined Policy Targeting:** Apply policies to collections, reducing manual effort.
 - **Scalability:** Collections automatically update as new computers meet the defined criteria.
 - Learn more about these new capabilities [here](#).

Identity and Federation

- **Enhanced Security with Duo Integration** (*in public preview*): Customers can enable Duo MFA for an extra layer of security during login and authentication, strengthening their security posture while ensuring a seamless user experience. Learn more about this new capability [here](#).
- **Improved User Experience with Extended Idle Timeout:** The maximum user idle timeout has been increased from 60 minutes to 12 hours.
- **Quick Account Unlock Option:** When users are locked out, Admins can now swiftly restore access to user accounts on the Delinea Platform.
- **New Documented Identity Providers for Federation:** Support has been added for Google, BlokSec, RSA ID Plus, and Celestix.
- Learn more about these new capabilities [here](#).

Platform Engine Management

- **Nomenclature Updates:** Consolidated naming across Engine Management and Platform Engine, including updates to UI, Engine installer, and documentation. Some of these changes will be seen iteratively over the coming months.
- **Improved Logging:** View all Platform Engine and workload logs directly in the Engine Management UI, enhancing supportability.
- Learn more about these new updates [here](#).

Integrations and Marketplace

- **Download Center** (*in public preview*): A dedicated space within the Delinea Marketplace. This new feature simplifies access to a wide range of downloadable resources, including agent updates and tools. Learn more about this new capability [here](#).
- **New and Updated Integrations:**
 - External Secrets Operator with Secret Server
 - MS Sentinel AMA Integrations with Secret Server CEF and Syslog
 - RabbitMQ Helper upgraded to have UI-guided install
 - Jenkins Release 1.0.9

- Terraform Secret Server Integration upgrade 2.0.8
- JDBC Proxy for Tomcat and WebSphere upgrade v3.3
- MidServer Credential Resolver 4.5.2
- Learn more about new integrations [here](#).

New Authenticator Mobile App

- **New Authenticator Mobile App** (*now in GA*): Introducing a dedicated mobile app for authentication. The app is now available in iOS and Google Play stores.
 - **QR Code Registration**: Users can scan a QR code to register.
 - **Push Notifications**: Receive authentication request notifications on your registered mobile device
 - **Renamed "Authenticator" Tab to "Passcodes"** in the Delinea Mobile application
 - **New Registration Workflow**: Implemented for all mobile applications on the Delinea Platform
 - **Now listed in the Platform Marketplace**
 - Learn more about this new application [here](#).

Other updates

- **Platform APIs** (*now published*): The Platform APIs provide developers with comprehensive access to key platform functionalities. The APIs allow seamless integration, automation, and customization to enhance your Delinea experience:
 - [Platform API Documentation](#)
 - [Sample PostMan Collection](#)
 - Sample scripts ([PowerShell](#) and [Python](#)) to manage OAuth tokens and test API connectivity for the Delinea Platform. These are simplified examples and might need to be adapted to fit your specific requirements.
- **Platform Service Account**: When you create a service account on the platform, an application account in Secret Server Cloud will now be created automatically, without the need to log in with the service account iteratively.
- **Delinea Expert** (*in public preview*): Delinea Expert is a secure, conversational AI designed to understand and generate human-like text using curated Delinea knowledge. Users can ask questions about platform features, components, or best practices and receive answers with supporting links. Learn more about this new capability [here](#).
- **Webhooks** (*in public preview*): Supports sending platform audit logs to an HTTP webhook endpoint with enhanced event filtering, new webhook logs for better visibility and troubleshooting, and an updated UI for a streamlined experience. Learn more about this new capability [here](#).
- **Tenant IP Restriction**: This new feature enhances the security of your tenant by ensuring that only trusted IP addresses can connect, helping to protect sensitive data and operations. Customers can submit a Delinea support case with their desired IP ranges to apply to their platform tenant.
- **Web Password Filler** (WPF): Support for Manifest v3 as of version 3.10. Learn more about this update [here](#).

- **Enhanced Filtering Experience:** Updated filtering across all platform tables. This feature can be activated using the new user opt-in option under the user's profile preferences, or directly via the tables.
- **Expanded Favorites Functionality:** The *recents* and *favorites* table on the homepage now covers a wider range of objects on the platform, such as pages, secrets, and computers.

Summer (Q3) 2024 Release

Secret Server on Platform

Entra ID Password Changing

- **Alternative to Azure AD PowerShell Modules:** Introduced support for Microsoft Graph API to replace the retired Azure AD PowerShell modules.
- **MFA-Enabled Entra ID Account Passwords:** Added functionality to change passwords for Entra ID accounts with MFA enabled.
- **New Secret Templates:**
 - **Entra ID Application Registration:** Allows for containing and mapping an Entra Application as a privileged account for password changing, using the new OAuth Application Registration extended mapping.
 - **Entra ID User Account:** Enables password changing for an Entra ID account, even with MFA enabled, using the Application Registration.

Remote Access Service (RAS)

- **Rebranding:** Remote Access Service (RAS) has been rebranded to Privileged Remote Access (PRA).
- **Dark/Light Mode Themes:** Now supports dark and light mode color themes, matching the preferences applied to the platform.
- **RemoteApp Assets (Private Preview):** Introduced desktop applications as a first-class inventory object for providing just enough access.
- **File Transfer Usability improvements:** Multiple file uploads and downloads and background file transfers to ensure users can continue to work uninterrupted remotely.
- **Accessibility support:** All PRA menu operations can be accomplished using keyboard controls.
- **Clipboard masking:** Copy confidential information into the PRA clipboard minimizing exposure of sensitive data.

Connection Manager (CM)

Available in Connection Manager 2.5.2 Release

- **Vault Auto-Reauthentication Configuration:** Users can now configure the vault reauthentication behavior. Options include maintaining the existing behavior that automatically restarts the authentication flow or forcing a fresh login when vault session/refresh tokens expire. This feature is especially beneficial for users with longer session/refresh lengths configured through an external identity provider.

- **Machine Field Display:** Connection Manager now displays a "Machine" field from Secret Server, helping users identify the correct target when the secret name is not self-explicit. This field will show in both the Secret Server and Connection Manager grid views.
- **Session Status Popup:** The Session Status popup window, which appeared every time a user signed out of a vault, is now disabled by default. Users can re-enable this pop-up if they encounter memory leak issues.
- **Memory Leak Resolutions:** Addressed various memory leaks to improve performance.

Identity & Federation

- **MFA for Federated Users (now GA):** Federated users can now be challenged for additional MFA within the Platform, including Platform user logon and browser-based step-up MFA such as secret access.
- **Identity Policies Administration:** Significant UX improvements for creating and managing identity policies, including better handling of default values and the flexibility to apply policies globally or to specific groups.
- **Bulk Invite Users:** Administrators can now invite users in bulk from various identity directories, including Delinea and Active Directory (AD). This feature covers AD users who have not yet logged into the platform.
- **New Connector v6.1.350:** Improved the Delinea Connector with a job to refresh "EnvironmentInfo", periodic updates for AD Topology, adjusted refresh intervals based on user changes, and a fix for AD master node syncing issues. Note: Upgrade to v6.1.350 or later by August 31, 2024, to avoid downtime due to major API changes.
- **New Documented Identity Providers for Federation:** Added support for AD FS, Entrust, and OneLogin.

Audit

- **Audit Logging:** Audit logging now supports audit events from various services including Identity, Inventory, and Tenant Profile (tenant customization).
- **Deep Linking:** Added support for deep linking within audit events to easily access users and session recordings.
- **Session Recording Comments (Private Preview only):** Users can now add and reply to comments on each session recording and flag risks.
- **AI-Driven Audit (Private Preview):** Improved AI-driven audit with streamlined call-to-action to run the analysis and a progress indicator.

Permissions

- **Consistency Across Platform Services:** Improved consistency for a more intuitive user interface by leveraging the same Add Member component as Identity.
- **Case Insensitivity:** Users can now search for permissions regardless of case sensitivity.
- **Enhanced Error Messages:** Improved error messages to assist with better troubleshooting.
- **Service Resiliency:** Enhanced resiliency to ensure more reliable performance.

Engine Management

- **Engine State Monitoring:** The engine state is marked as *Unknown* if the engine management does not receive a heartbeat within a specified time.
- **Uninstall Process:** The uninstall process now correctly displays the engine version.
- **Deleting an Engine:** Deleting an engine now clears all associated folders and removes old heartbeats.
- **Default Settings for Workloads** added.
- **All engine pool logs (including workload logs) now stored in:** C:\ProgramData\Delinea Engine\log.

Marketplace & Integrations

- **New Certification Badge, *Delinea Trusted*:** Indicates an integration maintained by a third-party vendor. While Delinea confirms its compatibility, ongoing support should be sought from the vendor's documentation or support channels.
- **Integration Configuration:** Simplified launch into configuring native integrations with a *Configure* button directly from the integrations themselves. This feature is utilized by various integrations, including identity providers for setting up federation providers, among others.
- **ITP/PCCE Integrations:** Introduced new integrations pertaining to Identity Threat Protection and Privilege Control for Cloud Entitlements.
- **New and Updated Integrations:**
 - All ServiceNow integrations certified for the Washington DC release.
 - MID Server Release 4.5.1
 - JDBC Proxy Driver 3.1/3.2 updated to utilize a new encryption method using hardware details to encrypt credentials.
 - Rapid7 Insight VM RPC can now be used as RPC with added scripts available in the *delineaxpm* GitHub repo.
 - SCIM Release 4.5.1 for Secret Server only
 - RabbitMQ Helper 10.5.0
 - Okta and ServiceNow OOB RPC in Secret Server
 - MS Sentinel AMA Connector Release for Secret Server
- **Security Upgrades:** Upgraded several packages to resolve security vulnerabilities, including:
 - SCIM Release 4.5.1
 - Terraform 2.0.6

New Authenticator mobile app

- **New Authenticator Mobile App (Private Preview):** Introducing a dedicated mobile app for authentication.
- **QR Code Registration:** Users can scan a QR code to register.
- **Push Notifications:** Easy-to-use push notifications.

- **Authenticator Tab Renamed to Passcodes:** The passcode function remains unchanged.
- **New Registration Workflow:** Implemented for all mobile applications on the Platform.

Other updates

- **Updated User Profile:** Enhanced user profile management to include account, security, and application preferences in one place, offering an improved user experience.
- **Global Platform Search (GA):** The global platform search feature is now generally available.

Spring (Q2) 2024 Release

Secret Server on Platform

QuantumLock: Quantum Safe Kyber encryption to secrets

- Prepare sensitive secrets for the growing risk of Quantum Computing.
- Defend against "Harvest Now - Decrypt Later" attacks.

Privileged Remote Access (PRA)

- Background multi-file uploads: Queue files for upload, continue remote work while files transfer in background automatically.
- File Transfers to RDP targets.
 - Support for SMB (v2 & v3) with Windows targets.
 - If both SFTP and SMB services are available on the target, PRA will use SFTP (more secure overall). If only SMB is available, PRA will automatically use it instead.
- Keyboard layout support: Easily switch keyboard layouts to match the keyboard layouts configured on target machines.
- Session Connector
 - Configure essential applications for PRA users and limit access to only what's needed
 - Inject Secret Server credentials into running applications
- Connection Info: Access to connection information (such as engine in use, target machine, etc.) for easy identification and troubleshooting when needed.
- Accessibility Improvements: Keyboard can activate and operate PRA menu during remote connections.
- Masked Clipboard for Sensitive Content: Mask sensitive content when using clipboard for data exchange.

Connection Manager (CM)

External Browser Authentication enables users to authenticate to the Delinea Platform through an external browser. This feature facilitates the reuse of existing log-ins, password managers, and advanced functionalities such as biometric MFA, FIDO2 support, and conditional access configurations with their chosen identity provider.

Inventory

Inventory is now generally available, offering users a new interface to view and remotely connect to target machines, utilizing:

- My Account: Users can log in to enrolled Linux systems with their Delinea Platform account, either via the platform or through native applications using SSH, SCP, or SFTP.
- Vaulted Credentials: Users can access any target system in the Delinea Platform using vaulted credentials from Secret Server.
- Manually Entered Credentials: Users can manually log in to target systems with valid username and password.

Audit

- Audit Logging is now generally available, supporting audit events from various services:
 - Secret Server
 - Privileged Remote Access
 - Permission Service
 - Audit Collector (included in Privilege Control for Servers)
 - Policy Service
 - Federation Service
- Sharing of recordings: Share links to recordings (with specific timestamps) with other users on the platform.
- Terminate Live Remote Sessions: Available for Privileged Remote Access and Secret Server.

Marketplace & Integrations

- Launch of the Delinea.com [Integrations Center](#)
- Addition of Community-provided integrations: These are scripts developed by external contributors and hosted on [Delinea's GitHub repository](#). They are not officially maintained by our development team and are provided "as is" with no guarantees on performance or compatibility.
- New and updated integrations:
 - SNOW MID Server 4.5
 - JDBC Proxy Driver 3.0
 - Rapid7 Insight VM Integration with Secret Server for Shared credential Sync
 - SCIM Release 4.4.4
 - Terraform 2.0.4/2.0.5
 - UiPath 2.6.0
- New Download Center (currently limited to Privilege Control for Servers customers)
- Enhanced user experience:

Release Notes

- Updates to certification and vendor filters
- Improved support for light and dark mode
- Significantly increased the number of integrated vendors.

Identity & Federation

- Add bulk users to the local directory: This feature allows administrators to import a large number of user accounts simultaneously, streamlining the process instead of adding users manually to the Delinea Directory one by one.
- MFA for federated users (private preview): Federated users can be challenged for additional MFA within the platform: This includes platform user log on and any browser-based step-up MFA, such as secret access.
- Ability to map a large number (beyond the previous limit of 100) of identity provider groups to platform groups.

Platform Engine Management

- Platform Engine Management is now available for general use.
- Support for two Privilege Control for Server (PCS) workloads: Command Relay and Audit Collector.
- Engine auto-upgrade to new versions and remote uninstallation are now supported.
- Utilize vaulted accounts within workload management settings.

Privilege Control for Servers

Introduction of the 'Require Session Recording' rule to manage recording during endpoint login and privilege elevation via policy, ensuring that login or elevation is prevented if host-based recording is cannot be initiated.

Delinea Mobile App

In Delinea Mobile 2.3 release, Offline Caching was introduced, aligning with the existing feature in our Secret Server Mobile app. This release offers:

- Single Secret downloads
- Consolidated offline view
- Expiration indicator
- New “Download” filter
- Download indicators per secret

Web Password Filler (WPF)

TOTP support was introduced in 3.9 release. With this update, you can generate and copy TOTP codes directly from the WPF browser extension. The code length is adjustable by the admin and operates on a 30-second loop.

Other updates

- New navigation interface offers a use-case-centric view of our platform services, with content categorized to reflect service relationships. This enhanced experience offers:
 - Simplified navigation for common use cases.
 - Ability to access available pages without redirection.
 - Customizability with expanded/collapsed views.
 - Swift access to frequently used features.
- The global platform search (private preview) has been updated to deliver more results, encompassing Assets & Marketplace outcomes, along with content. Content searches now include page titles and descriptions, enabling streamlined access to most products from a single search query.
 - Access all items from a single-entry point, minimizing menu navigation.
 - Uncover pertinent configurations based on keyword searches.
- Improved uptime SLA for platform now 99.99%. More information can be found on <https://delinea.com/sla>
- New Trust Center - <https://trust.delinea.com/>
 - Get Trust Center Updates in your inbox.
 - Access compliance documents such as ISO 27001 and SOC2 reports.
 - Stay informed about published vulnerabilities and their fixes.
 - Submit and report vulnerabilities.

Winter (Q1) 2024 Release

Secret Server on Platform

- Ongoing UI conversion to the same modern development framework as the rest of the product (Angular), covering Launcher configuration, dependency configuration, Remote Password Changer, and Heartbeat configuration screens.
- Discovery now retrieves zone metadata and additional Active Directory attributes, enabling identification of discovered AD assets with Privilege Control for Servers data, export to, and matching within the Inventory service.

Privileged Remote Access (PRA)

- File transfer to and from SSH targets
- PRA engine host sizing guide
- PRA engine host hardening guide
- Private Preview - RemoteApp support
- Readiness for Privilege Control for Servers

Connection Manager (CM)

- Supports MacOS Sonoma
- Supports Privilege Control for Servers (PCS) MFA-on-endpoint for AD-Joined SSH targets
- Check out a secret for exclusive access and extend time from within CM

Audit

- Combine Secret Server sessions alongside Platform sessions
- User experience enhancement throughout for better usability, including deep linking to other resources.
- Improvements to the quality and performance of transcription and anomaly detection - now available in Private Preview.

Marketplace & Integrations

- Integrations expanded to include multiple new listings for federation to IDPs, with various updates to existing integrations like PowerShell and Terraform.
- By default, Marketplace View Permissions are accessible exclusively to admin users.

Identity & Federation

- The Federation underwent a comprehensive UX/UI redesign, simplifying the Identity Provider creation process by eliminating wizards, enhancing automation to minimize configuration overhead, and introducing clearer visual cues for mandatory user mappings.
- Connector version 5.1.8 has been released with enhancements focused on improving reliability, stability, and extensibility. While earlier Connector versions will continue to function without service disruption, registration or re-registration of these versions with the Platform after Feb 15, 2024, may not successfully complete. It is advisable to upgrade your Connector to version 5.1.8 or the latest before the specified date.
- The Authentication Profiles settings page has undergone a complete UX/UI overhaul, introducing a new "Description" field and eliminating pop-up screens for configuring settings.

Other updates

- "Use my Account" is now available as a launch option (only for Linux machines)
- New Platform tenants will experience "Unified Mode" for Roles and Permissions - one management plane for all permissions.
- Customers now have the option to participate in the Public Preview program, allowing them to personally explore, test, and offer feedback on new enhancements before the official General Availability (GA) release.

Fall (Q4) 2023 Release

Secret Server on Platform

- The General Availability (GA) of Step-up Multi-factor Authentication (MFA) for Secrets is now available.

Privileged Remote Access (PRA)

- Introducing enhanced control for PRA clipboard functionality access
- Improved troubleshooting with more specific and detailed error messages
- RemoteApp support has entered Private Preview, allowing isolation of remote access to individual applications, rather than the entire desktop.

Web Password Filler (WPF)

- Early Access is now available for WPF 3.7, featuring support for synchronizing recent and favorite secrets in Secrets.
- You can now search for any web secret directly from the Recent tab.

Connection Manager (CM)

- Support for step-up MFA for Secrets

Integrations and Marketplace

- Introducing global search capability within the platform
- Various improvements to content and layout
- New permissions have been added, including download and view permissions.
- Integration updates:
 - RabbitMQ: Now supports several new commands and the latest stable versions of Erlang and RabbitMQ
 - JDBC Proxy Driver: Offers support for multiple data sources and enhanced credential validation for WebSphere and Tomcat.
 - Ansible - RedHat Ansible Secret Server collection Certification
 - SCIM on premise: Upgrades include enhanced logging, role assignment additions, and updates to the configuration page.
 - UiPATH Orchestration on premise: Enhanced token expiration support for API calls, enabled retry functionality by default, and improved credential encryption.
 - SDK plugins - Addressed all Open vulnerabilities
 - ServiceNow: Upgraded ServiceNow MID Server Integrations, added support for SNMPv3 Credentials, and credential encryption utility.

Identity & Federation

- We now provide platform federation support for SAML and OIDC with Ping Identity (PingOne).
- IDP-initiated Single Sign-On (SSO) flow is now supported.
- Introducing the Federation Debug Console, a self-service debugging tool for troubleshooting federation setups with Identity Providers (IdPs).

- Third-Party MFA Servers (via Radius) now Generally Available (GA).
- We have introduced a set of documentation and example scripts on GitHub to automate the installation of the Delinea Connector.
- Introducing a new set of federation settings:
 - Customize Issuer Sent To IDP: This setting allows you to override the default Certificate Issuer (Entity ID) sent to the Identity Provider (IdP).
 - Request Binding: This setting controls the method for binding SAML authentication requests to the communication protocol.
 - Sign Request: This setting ensures that SAML authentication requests sent to the IdP are digitally signed for enhanced security.
- You can now verify the status of the Delinea Connector using the new Ping Connector capability.

Other updates

- Introducing new UX updates to the platform's user profile.
- Asset View is now available in Private Preview, offering users a new way to access inventory by machine and enabling remote session invocation.
- Improved roles and permissions: The Everybody group can now be removed from the Platform User role, providing greater permission customization.

Summer (Q3) 2023 Release

Secret Server on Platform

- MFA (Mufti Factor Authentication) on Secret access, now in Private Preview, is a new security mechanism designed to enhance the protection of sensitive credentials and privileged information stored within Secret Server's vault. MFA on Secret access helps ensure that only authorized individuals with the correct authentication factors can retrieve these valuable credentials.
- Improvements to Discovery UI and overall user experience

Privileged Remote Access (PRA)

- Additional logging and diagnosability to effectively identify and resolve issues
- Support for HTTPS PROXY by the PRA engine
- Support for remote access to target systems using Secret Server RDP proxy configurations

Web Password Filler (WPF)

- Web Password Filler v3.5.3: Users can now log in to their Delinea Platform tenant from WPF.

Connection Manager (CM)

- Connection Manager v2.0: Users can now log in to their Delinea Platform tenant from CM.

Audit

- Simplified, intuitive navigation for session recordings
- Enhanced playback controls: full screen and zoom features are now supported
- Improved responsiveness to live streaming and encoding processes
- Secret name now included and deep linked on the session recordings

Marketplace & Integrations

- This update brings a complete overhaul of the user experience for Marketplace:
 - Consolidated tabs for Applications and Tools and Integrations tabs
 - Both tabs now have dynamic filters relative to each tab which simplifies searching for specific or available integrations.
 - Marketplace cards have been updated to clearly identify Vendor, Integration name, supported Application, and certifications, for faster search.
 - Details pages have been redesigned to have more descriptive content.
 - Details pages no longer show full documentation, and instead link to the appropriate documentation articles.
- Integrations added or updated for Secret Server on the platform:
 - Palo Alto XSOAR v3.0.1: Introduces a new capability to allow users to add automated comments which will display under Secret Server Audit.
 - PowerShell Module v0.61.3: Updated the package to resolve the cryptography vulnerability and updated SS (Secret Server) SDK to v1.5.3.
 - UiPath v2.2.0: Resolved issues with multiple SDK accounts being created on a Secret Server. SDK account details are now stored in the config file (in encrypted format) in the user temporary directory.
 - Ansible plugin: updated to allow secrets calls by path and ID.
 - SCIM for Secret Server, Multiple Releases (Current v4.4.1): Streamlined integration with IGA providers, and resolved vulnerability issues.
 - RabbitMQ Helper, Multiple Releases (Current v10.2.0): addressed reported issues, and added the ability to upgrade RabbitMQ using a URL provided by the user.

Identity & Federation

- Simpler workflow for adding local users: This enhancement aims to streamline the process of creating new local users in the platform, by reducing the steps it takes, making it easier and more efficient for administrators.
- Visibility in users' platform login activities: log of all recent login activities associated with a user's account. This includes information such as date, time, source IP address, browser, and OS details of each login attempt.
- Third Party MFA Servers (via Radius), now in Private Preview. You can use your RADIUS server to authenticate users to the Delinea Platform. RADIUS authentication can be used with Multi-Factor Authentication (MFA) to provide an additional security layer.

- Delinea Connector auto-update support: you no longer need to manually download and install Delinea Connector updates. The platform can now automatically handle the update process in the background, ensuring that you always have the latest version of the connector without any effort on your part.
- Streamlined the user experience flow to download the Delinea Connector and generate its registration code.
- Force Re-authentication with Identity Providers (IdP): By default, federated users are not prompted to re-authenticate with IdPs every time they try to log on to the platform, assuming the user has a valid authentication session with the IdP. The introduction of this capability in platform helps where this experience may not be desired, such as on shared workstations and/or if re-authentication is required where sensitive operations are performed with requirements for governance and assurance.

Other updates

- Global Search: powerful search functionality empowers you to find everything you need across the platform. This capability is now limited to search across Secrets, with plans for further integration across the entire platform.
- Ability to dismiss the platform set up flow: you can now choose to skip the onboarding setup tasks, tailoring the onboarding process to your specific needs.

Spring (Q2) 2023 Release

New Hosting Regions

The Delinea Platform is now available globally in the following geos

- US
- Canada
- Europe
- Australia
- UK
- Southeast Asia

Behavioral Analytics (Private Preview)

Now in Private Preview, Behavioral Analytics is the next evolution of our standalone Privileged Behavioral Analytics, seamlessly integrated with everything on the Delinea Platform to showcase the power of a unified cloud-native platform. Highlights:

- ML-powered anomaly detection
- A user-friendly interface that makes it easy to get started with Behavioral Analytics
- Powerful data-visualization that helps to quickly identify anomalous patterns and potential risks

Contact your Sales rep if you'd like to try it before GA.

Permissions Service

- This new service helps platform administrators define roles and assign specific permissions to each role.
- Users or groups can then be assigned to these roles, thus inheriting the expected defined privileges.
- This service allows for a flexible and scalable way to manage access controls and ensures that only authorized users have access to sensitive resources.
- Supports both custom and built-in roles
- Offers fine-grained controls over access to resources
- Simplified UX to manage roles and permissions

Improved Home Screen

- Complete UI overhaul of the platform home screen
- Added a new platform onboarding task list

Marketplace

- The New Delinea Marketplace is your one-stop shop for Delinea applications, partner integrations, and direct downloads.
- Dynamic Category Search Drop-Down is now available
- Many new integrations added, including Microsoft Sentinel and ConnectWise Control
- Mobile App has been added

Tenant Customization

Customers can now update the look and feel of the platform tenant portal to suit their corporate branding.

Features:

- Add custom terms/privacy notices
- Add company name
- Add corporate logo (dark/light mode support)
- Set banner
- Username format/display hint

Winter (Q1) 2023 Release

Seamless Integration with Secret Server Cloud

Existing Secret Server Cloud users can view and manage secrets entirely within the Delinea Platform with a familiar user experience. Users can fully leverage the platform as their primary interface for their day-to-day use of Secrets

Next-Gen Privileged Remote Access

- Launch secure VPN-less browser-based SSH and RDP sessions with a single click
- Agentless deployment – no additional software is required on target hosts
- No end-user clients required – based on a modern HTML5-based web client
- Zero impact on customer security posture – no inbound firewall rules to open
- Agentless session recording to meet customers' audit and compliance requirements

Robust Identity and Federation Services

- Support for Active Directory
- OIDC Federation, SAML support
- Policy-based MFA (including FIDO2, Passkey, etc.) for platform login

Marketplace

The New Delinea Marketplace is your one-stop shop for Delinea applications, partner integrations, and direct downloads.

Foundational Shared Services

A wide range of unified services such as authentication, notification, and federation services.

SMS Terms of Service

1. This service will provide messages to allow multi-factor authentication (one-time codes sent via SMS) to end-users into the Delinea Platform.
2. SMS notifications are managed within the Delinea Platform and are subject to your organization's administrative policies and procedures.
3. START/STOP/HELP messages are supported via SMS. STOP message may impact your ability to continue receiving verification codes to log in to the Delinea Platform. For HELP please contact your organization's Administrator.
4. If you are experiencing issues with these messages, you can get help directly from support@delinea.com or by calling +1(202) 991-0540.
5. Carriers are not liable for delayed or undelivered messages
6. Message and data rates may apply.
7. If you have any questions regarding privacy, please read our privacy policy: <https://delinea.com/privacy-policy>

Local File Locations

This topic lists the standard Windows locations for Delinea files.

Path	File(s) or File Type	Notes
C: Program Files\Delinea\Delinea Connector\	Log files for the Delinea Connector	
C: Program Files\Delinea Engine\[version-number]\	appsettings.json	Edit as administrator to increase the level of engine log details to Debug.
C: ProgramData\Delinea Engine\log\	All Engine Management and engine workload log files	
	audit-collector_[version-number].log	Log file for the Audit Collector engine workload
	command-relay_[version-number].log	Log file for the Command Relay engine workload
	remote-access-service_[version-number].log	Log file for the PRA engine workload
	Platform.Engine.Bootstrap_[version-number].log	Log file for engine startup flow logic
	Platform.Engine.Default_[version-number].log	Log file for engine runtime and process information, including updates from the platform's Engine Management service, starting and ending deployments, and heartbeats sent to the platform.
	Platform.Engine.Registration.EnginePool_[number].log	Log file for Engine Management
	Platform.Engine.Registration.Platform_[number].log	Log file for the engine registration process

Path	File(s) or File Type	Notes
	Platform.Engine.SelfUpgrade_[number].log	Log file that exists if the engine has begun an upgrade attempt
C: ProgramData\Delinea Engine\[version-number]\	Encryption key files for engine and workload files	
appdata\	key-[number] encryption key file	For encrypting engine configuration files
appdata\settings\	key-[number] encryption key file	For encrypting engine option, deployment, connection, upgrade, and uninstall files
C: ProgramData\Delinea Engine\[version-number]\deployment\delinea\	Encryption key files for workload files	
delinea-audit-collector\[version-number]\	key-[number] encryption key file	For encrypting Audit Collector deployment state files
delinea-command-relay\[version-number]\	key-[number] encryption key file	For encrypting Command Relay deployment state files
delinea-remote-access-service\[version-number]\	key-[number] encryption key file	For encrypting Privileged Remote Access deployment state files

Glossary

Access Explorer

A platform UI page (Inventory > Access Explorer) that displays visual representations of the relationships between identities, assets, and access policies, based on the filters and sources selected. You can use the Access Explorer to find out how an identity gains

access to an asset, which identities have access to an asset, or when access or membership was granted.

Active Directory (AD)

Active Directory (AD) is a proprietary directory service developed by Microsoft® to manage the authentication and authorization of users and machines on a Windows domain network. Active Directory runs on Windows Server and stores information related to user accounts, computer objects, groups, policies, and other entities on the network.

AD

Active Directory (AD) is a proprietary directory service developed by Microsoft® to manage the authentication and authorization of users and machines on a Windows domain network. Active Directory runs on Windows Server and stores information related to user accounts, computer objects, groups, policies, and other entities on the network.

Agent

An agent is software installed on a computer that can act autonomously to achieve goals set by humans. An agent has self-governing attributes and capabilities in reasoning, learning, adaptability, decision-making, policy-following, and execution.

Audit

A record of actions that are typically user initiated but may also include some system actions. An audit is designed for consumption by users - mainly security overseers like SecOps and CISOs.

Audit Collector Workload

A workload run by the delineate engine that enables Privilege Control for Servers (on the delineate platform) to receive audit data about events and actions during session recording captured by the privilege control agent deployed on audited computers. More than one delineate engine and Audit Collector workload can be deployed for greater resilience and/or scale. Minimum requirement: two Audit Collector workloads to ensure uninterrupted auditing.

Authentication

Authentication is a way for a user to prove that they are still the person they claimed to be during the identification phase by inputting something a person knows, such as a

password or security question; something a person has, such as a token, smartcard, ID card, or cryptographic key; or something a person "is," using biometric data such as a fingerprint or facial scan.

Authentication Challenge

A mechanism on the Delinea Platform to challenge a user attempting to log in. Examples include password, phone call, email confirmation code, and security questions.

Authentication Profile

On the Delinea Platform, an authentication profile specifies the authentication challenges required to log in to the platform and the length of time that must elapse before a user is prompted for authentication again.

Authorization

Authorization is the process of verifying what specific applications, files, and data a user has access to.

Birthright User Type

In IGA/ILM, Birthright access is granted to every Identity of this user type and can never be removed. An example might be an email account for employees. All identities of the Employee User Type are granted an email account and they have that email account as long as they are an employee.

Catalog

In IGA/ILM, a Catalog is a collection of accesses that are made available for users to request. Each catalog is associated with a User Type. When an Identity accesses self-service, they can request any access that is available their User Type AND that is in a catalog associated with their User Type.

CID

Continuous Identity Discovery (CID) extends the discovery capability of Secret Server Cloud on the Delinea Platform to cover cloud identities, including privileged accounts, service accounts, admins, and shadow admins.

CIEM

Cloud Infrastructure Entitlement Management (CIEM) is a security approach for controlling access rights to cloud resources. CIEM solutions identify all existing privileges across cloud and multi-cloud environments, then identify privileges that are

higher than they should be, such as privileges that are stale and no longer needed to help reduce the risk of unauthorized access.

Cloud Infrastructure Entitlement Management (CIEM)

Cloud Infrastructure Entitlement Management (CIEM) is a security approach for controlling access rights to cloud resources. CIEM solutions identify all existing privileges across cloud and multi-cloud environments, then identify privileges that are higher than they should be, such as privileges that are stale and no longer needed to help reduce the risk of unauthorized access.

cloudadmin

A local Delinea Platform “break-glass” account that is created for you. It follows the format `cloudadmin@your_platform_tenant_name`. `cloudadmin` is the first account you need to perform initial platform provisioning, login, integration, and setup tasks.

Collection

A collection is an inventory query that is saved for future reuse. A collection can also be used to build custom dashboards, detection rules, and scheduled reports. All collections on the platform are automatically updated daily and can also be updated on demand. In IGA/ILM, a Collection is a grouping of items of the same type that can be used throughout the application. In addition, Ownership Collections define who owns which items for use with certification and approvals. A collection can support the following types of items: Role, Resource, Entitlement, Company, Identity. Each collection type EXCEPT Identity can have owner(s) assigned to each collection Item. The owner can be defined as an identity or a collection of identities.

Command Relay Workload

A workload run by the platform engine that enables Privilege Control for Servers to send commands and parameters through an SSH connection for execution on a customer’s servers. The Command Relay workload depends on a service account that can modify the Active Directory domain to update policies.

Continuous Identity Discovery (CID)

Continuous Identity Discovery (CID) extends the discovery capability of Secret Server Cloud on the Delinea Platform to cover cloud identities, including privileged accounts, service accounts, admins, and shadow admins.

Data Type

In IGA/ILM, a field has a data type that defines the type of information stored.

Default Granted User Type

In IGA/ILM, Default Granted access is granted to every Identity of the user type when the Identity is created (or changed to that user type), but the access can be removed.

Default not Granted User Type

In IGA/ILM, Default Not Granted means that access is not granted to new identities by default, but it could be added. Default Not Granted access could be added directly by Administrators or Manager, it could be added by policies attached to a role, or it could be added through a self service request if the access is available in a catalog.

Delinea Connector

The Delinea Connector enables secure communication between the Delinea Platform, Active Directories, and various services within your internal network. For enhanced reliability and efficiency, it is recommended to deploy multiple Connectors to enable failover capabilities and load distribution.

Delinea Expert

A secure AI chatbot that answers questions about the Delinea Platform's features, components, or best practices, and provides links to support its answers. Delinea Expert cannot access your data or see which platform page you are on. Delinea Expert can sometimes make mistakes – always check important information. If an answer seems inaccurate, please click the Flag icon to alert us.

Distributed Engine

An engine used by secret server on platform, secret server cloud, and secret server on-premises to take actions in the customer environment and update secrets. In the future, secret server on platform will use only the Platform Engine for these actions.

Dynamic Collection

In IGA/ILM, Roles can be automatically assigned to users by Dynamic Collections. The role will be assigned to any user in the dynamic collection. Dynamic collections are evaluated when user is created, when user is updated, on a schedule, when the collection definition is updated, and when a user type is updated.

Dynamic Collections

In IGA/ILM, Roles can be automatically assigned to users by Dynamic Collections. The role will be assigned to any user in the dynamic collection. Dynamic collections are evaluated when user is created, when user is updated, on a schedule, when the collection definition is updated, and when a user type is updated.

Engine Management

A platform UI page (Settings > Engine Management) where admins manage Platform Engines, the Sites where the engines are deployed, and the Workloads that the engines run.

Engine Site

A group of engines selected on a common principle, e.g. network or subnet, or geographical location (office, city, etc.), or data center, or any other characteristics that the IT personnel finds appropriate. Workload settings are organized at the Engine Site level.

Engine Workload

A background service managed and deployed by Delinea, provisioned and run by Platform Engines, and configured by administrators in Engine Management. Engine Workloads include Audit Collector, Command Relay, PRA, and ITP for Active Directory. Workloads are updated automatically by the Engine when a new version of the workload is available. Other independent Engines (such as Distributed Engine) or Connectors will over time be converted into workloads to be downloaded and provisioned by the Delinea Engine as necessary.

Entitlement

In IGA/ILM, Entitlements are the application roles (security roles, responsibilities, security groups, permission sets, etc.) accessed within a Resource.

Field

In IGA/ILM, an identity is based on a default set of fields. Customers often need to configure how identity information is managed, and track additional information about the identities they manage. All standard fields are configurable, and custom fields allow customers to extend the definition of an Identity and store what information is essential based on their business needs. Fields provide metadata about individual data fields on business objects such as identities, resources, roles, and entitlements. The metadata will describe the contents and validation of the field. When a field is associated with an

object type, data can be set in that field for specific instances of that object type. Fields are used to describe intrinsic, or built-in, elements of an object as well as custom extensions to that object.

Form

In IGA/ILM, Forms are used to update identity data in Delinea IGA. Form customization allows customers to create forms by adding fields that capture the data needed to manage their identities. Identity Creation Forms: These forms will be used by administrators and/or managers to create identities in the system. Identity Update Forms: These forms will be used by administrators and/or managers to update existing identities in the system.

Identity

Identity is the process of identifying a particular user, usually by providing a name, email address, phone number, or username. This is the process of someone saying that they are a certain person. In IGA/ILM, an Identity is created when a new person is entered into the relevant HR system, and that information triggers birthright access to an Identity Access Management system (such as Okta or Entra ID).

Identity Governance Administration (IGA)

On the Delinea Platform, Identity Governance Administration (IGA) empowers platform administrators to secure their organization by managing access to information, systems, and resources, ensuring the correct individuals (employees, contractors, or partners) have appropriate access to the correct resources at the correct times, and properly monitoring and auditing their access. Access management is automated based on the organization's specific setup and configuration of Identity Governance and Administration (IGA).

Identity Lifecycle Management (ILM)

The processes (Joiner, Mover, Leaver) are key components of Identity Lifecycle Management, which ensures secure and appropriate access throughout the identity's lifecycle in an organization.

Identity Policy

An identity policy determines whether and when a Delinea Platform user is presented with the challenges specified in the associated authentication profile.

Identity Threat Protection (ITP)

Identity Threat Protection (ITP) solutions safeguard identities and the systems they access by detecting and preventing identity-based threats like malicious insiders, account takeovers, and privilege escalations.

IGA

On the Delinea Platform, Identity Governance Administration (IGA) empowers platform administrators to secure their organization by managing access to information, systems, and resources, ensuring the correct individuals (employees, contractors, or partners) have appropriate access to the correct resources at the correct times, and properly monitoring and auditing their access. Access management is automated based on the organization's specific setup and configuration of Identity Governance and Administration (IGA).

ILM

The processes (Joiner, Mover, Leaver) are key components of Identity Lifecycle Management, which ensures secure and appropriate access throughout the identity's lifecycle in an organization.

ITP

Identity Threat Protection (ITP) solutions safeguard identities and the systems they access by detecting and preventing identity-based threats like malicious insiders, account takeovers, and privilege escalations.

Joiner

In IGA/ILM, a Joiner is an identity added to or newly created in a system. Depending on the organization's specific needs, this identity could represent an employee, contractor, or even equipment. At this stage, appropriate access permissions must be assigned based on the role of the identity being onboarded.

Leaver

In IGA/ILM, a Leaver is an identity removed from the system, typically upon termination of employment or the end of a contract. The removal can be manual or pre-scheduled, particularly in cases where access is time-bound. It is important to ensure that all access permissions are revoked to prevent unauthorized access after the individual has left.

Log

A record of background events typically related to systems, performance, outages, etc. A log is typically consumed by IT/Ops to help them ensure that things are running optimally and delivered according to the appropriate SLA.

Marketplace

The Delinea Platform Marketplace is an integration ecosystem for shared services where you can find applications, scripts, utilities, and other software that you can use with the Delinea Platform. By default, the Admin User role has access to Marketplace and they can control Marketplace access permissions for users.

MFA

Multi-factor Authentication (MFA) adds an extra layer of security by requiring users to prove their identity using two or more different factors, such as something they know (like a password), something they have (like a phone or security token), or something they are (like a fingerprint or facial scan). Even if a password is compromised, MFA can prevent unauthorized access because the attacker would still need to obtain the additional verification methods.

MFA for Secrets

Multi-factor Authentication (MFA) for secrets gives Delinea Platform administrators the option to add one or more security requirements to access specified secrets. This functionality is available exclusively through the Delinea Platform and supports many types of MFA, such as email, the Delinea Mobile App, YubiKey, and other devices using the FIDO2 protocol.

Mover

In IGA/ILM, a Mover is an identity that changes, such as an employee moving to a new role or department or a contractor transitioning to a full-time employee. It is crucial during this stage to ensure that only the necessary permissions for the new role are retained, as retaining previous access in combination with new permissions can lead to security risks.

Multi-factor Authentication

Multi-factor Authentication (MFA) adds an extra layer of security by requiring users to prove their identity using two or more different factors, such as something they know (like a password), something they have (like a phone or security token), or something they are (like a fingerprint or facial scan). Even if a password is compromised, MFA can prevent

unauthorized access because the attacker would still need to obtain the additional verification methods.

PCCE

Delinea Privilege Control for Cloud Entitlements (PCCE) discovers privileged identities across complex multi-cloud environments, identities and fixes identity misconfigurations and enforces the principle of Least Privilege access.

PCS

Privilege Control for Servers (PCS) carries the PAM capabilities of the Delinea Platform into the individual servers and computer endpoints in your corporate network.

Platform Admin

A Delinea Platform role with extensive permissions that is automatically assigned to all members of the System Administrator group.

Platform Engine

Software installed on servers in a network segment (a Site) that enables the Delinea Platform to perform various actions on that network via Workloads, such as discovery, remote access, authentication or session recording collection. The Delinea Engine acts as a single installer that will dynamically deploy the workloads as needed. For redundancy and high availability, admins can deploy two or more Platform Engines per site.

PRA

A feature of Delinea Platform that enables secure remote access to computers that is audited and session recorded. Formerly Remote Access Service (RAS).

Privilege Control for Cloud Entitlements (PCCE)

Delinea Privilege Control for Cloud Entitlements (PCCE) discovers privileged identities across complex multi-cloud environments, identities and fixes identity misconfigurations and enforces the principle of Least Privilege access.

Privilege Control for Servers (PCS)

Privilege Control for Servers (PCS) carries the PAM capabilities of the Delinea Platform into the individual servers and computer endpoints in your corporate network.

Privileged Remote Access (PRA)

A feature of Delinea Platform that enables secure remote access to computers that is audited and session recorded. Formerly Remote Access Service (RAS).

RBAC

Role-Based Access Control (RBAC) is the process of mapping access permissions to organizational roles, essentially to define what an individual is allowed to have access to if they have a particular role or roles within the organization. RBAC is important when designing an IGA implementation, as it enables you to make sense of all the varied access requirements across the organization and prevent access from being a 'free for all'.

Resilient Secrets

A feature of secret server on platform, secret server cloud, and secret server on-premises that duplicates all secrets and configurations from one secret server (the source) to a backup store (the replica). The feature is officially called Resilient Secrets, but the UI says Disaster Recovery.

Resource

In IGA/ILM, a Resource is an item a user can be granted access to within an organization. This could be a physical asset, such as a key card or an application, such as Ping Directory, Okta, Entra ID, and so forth.

Role

In IGA/ILM, A Role is a collection of resources and entitlements, and can be assigned as a group. Roles are organized around the access required for a specific purpose, such as a job role with the access needed to perform a specific job function.

Role-Based Access Control (RBAC)

Role-Based Access Control (RBAC) is the process of mapping access permissions to organizational roles, essentially to define what an individual is allowed to have access to if they have a particular role or roles within the organization. RBAC is important when designing an IGA implementation, as it enables you to make sense of all the varied access requirements across the organization and prevent access from being a 'free for all'.

SCIM

System for Cross-Domain Identity Management (SCIM) is an open standard that automates the exchange of user identity information between systems. It's used to manage user accounts and access to cloud-based applications.

Secret

A piece of information that is stored and managed in the Delinea Secret Server vault. Typical secrets include privileged passwords on routers, servers, applications, and devices. Files can also be stored in secrets, such as private key files, SSL certificates, license keys, network documentation, Microsoft Word or Excel documents, and more. Secrets are derived from secret templates.

Secret Server

The Delinea secrets vault. Delinea Secret Server is an enterprise-grade secrets storage vault for securely storing, managing, and controlling access to privileged credentials and other sensitive data. See Secret Server on Platform, Secret Server Cloud (SSC), and Secret Server on Premises (SSOP) for distinctions.

Secret Server Cloud (SSC)

Secret Server Cloud (SSC) is the Delinea secrets vault deployed from the cloud. Customers who purchased Secret Server Cloud before November 2023 must perform integration procedures to manage receive Secret Server on Platform as a fully integrated component of the Delinea Platform. See Secret Server on Platform and Secret Server on Premises (SSOP) for comparisons.

Secret Server on Platform

The Delinea secrets vault deployed from the cloud, fully integrated with and managed from the Delinea Platform. All customers purchasing Secret Server after November 2023 receive Secret Server on Platform as a fully integrated component of the Delinea Platform. See Secret Server Cloud (SSC) and Secret Server on Premises (SSOP) for comparisons.

Secret Server on Premises (SSOP)

Secret Server on Premises (SSOP) is the Delinea secrets vault installed on a customer server (instead of the cloud). Secret Server on Premises (SSOP) can be connected to the Delinea Platform as a limited integration to enable customers to launch PRA from a secret. It does not enable any other Secret Server functionality from the Delinea

Platform. See Secret Server Cloud (SSC) and Secret Server on Platform for comparisons.

Secret template

Secret templates are used to create secrets and allow customization of the format and content of secrets to meet company needs and standards. Examples include: local administrator account, SQL Server account, Oracle account, credit card and Web password. Templates can contain passwords, usernames, notes, uploaded files, and drop-down list values. All existing templates can be modified, and new secret templates can be created.

Shadow Administrator

Shadow Administrator accounts have sensitive privileges assigned to them directly (and not through membership in an administrator's AD group) that can allow them to take over other privileged accounts and leverage them to reach their target systems to compromise them. Shadow Administrator accounts present security vulnerabilities.

SSC

Secret Server Cloud (SSC) is the Delinea secrets vault deployed from the cloud. Customers who purchased Secret Server Cloud before November 2023 must perform integration procedures to manage receive Secret Server on Platform as a fully integrated component of the Delinea Platform. See Secret Server on Platform and Secret Server on Premises (SSOP) for comparisons.

SSOP

Secret Server on Premises (SSOP) is the Delinea secrets vault installed on a customer server (instead of the cloud). Secret Server on Premises (SSOP) can be connected to the Delinea Platform as a limited integration to enable customers to launch PRA from a secret. It does not enable any other Secret Server functionality from the Delinea Platform. See Secret Server Cloud (SSC) and Secret Server on Platform for comparisons.

System Administrator

Platform users who belong to the System Administrator group inherit the Platform Admin role, with extensive administrative permissions. The System Administrator group cannot be renamed or deleted. Compare to cloudadmin.

System for Cross-Domain Identity Management (SCIM)

System for Cross-Domain Identity Management (SCIM) is an open standard that automates the exchange of user identity information between systems. It's used to manage user accounts and access to cloud-based applications.

Task

In IGA/ILM, Tasks are the discrete units of work that are assembled to compose a workflow. There are two basic task types: User Tasks and System Tasks. User Tasks are accomplished by human users. User tasks require one or more assignees, and when a workflow reaches such a task, the assignee(s) are notified. In some cases, a task may be delegated by an assignee to one or more delegates who will complete the task instead. System Tasks are automatically accomplished by system processes.

User Type

In IGA/ILM, a User Type defines a large grouping of similar users. It can be viewed as a 'big bucket' of users with much in common, even though they don't all have the same business role. Typical examples include staff, contractors, customers, and students. User types could also be used to group users in particular geographies, such as US and UK staff. User types are helpful not only for classifying users but also for provisioning access. One way is by assigning items through Birthright access at the user type level.

User Type Access Model

In IGA/ILM, the User Type is the basis for the Identity Access Model. Each Identity has exactly one User Type. The User Type defines the initial access given to an Identity, and the potential access that an Identity could have.

View

In IGA/ILM, Views are used to display data in Delinea IGA. Identity Display Views: Used by administrators and/or managers to view existing identities in the system. Identity Flyout Views: Used by administrators and/or managers to get a quick view of additional information for existing identities on the Identities Inventory page.