Delinea Platform

Administrator Guide

Version: 2024

Publication Date: 5/18/2024

Delinea Platform Administrator Guide

Version: 2024, Publication Date: 5/18/2024

Table of Contents

Administrator Guide ... 1

Welcome to the Delinea Platform ... 1

Navigation ... 1

Introduction to the Delinea Platform ... 1

Benefits ... 1
Features ... 1
Secret Server ... 1
Remote Access Service ... 2
Privilege Control for Servers ... 2
Identity Threat Protection ... 2
Privilege Control for Cloud Entitlements ... 2
Robust Identity and Federation Services ... 2
Built-in Delinea Marketplace ... 3
NextGen Mobile Application ... 3
Getting Started ... 3
Overview ... 3
General Tips ... 3
1. Provision and Log into the Platform ... 4
For Current Secret Server Cloud Customers ... 4
For New or Prospective Delinea Customers ... 5
For Current Secret Server On-Premise Customers ... 5
2. Add Domain User Accounts ... 5
2a. Add Active Directory User Accounts ... 6
2b. Add Federated User Accounts ... 6
Local User Acounts ... 7
3. Assign Yourself Admin Permissions and Access Secrets ... 7
3a. Assign Platform Admin Permissions to Your Personal Domain Account ... 7
3b. Assign Secret Server Admin Permissions to Your Personal Domain Account ... 7
3c. Access Secrets from the Platform ... 8
Link Platform and Secret Server Groups ... 8
Sync Platform and Secret Server Groups ... 9
Assign Secret Server Permissions to Platform Users ... 9
Automatically Create Groups During Synchronization ... 10
Set Up and Use Remote Access Service ... 10
Launch a RAS Session ... 10
Assign Roles and Permissions to Users and Groups ... 11
Onboarding Troubleshooting ... 11
Finding Your Delinea Support PIN ... 11
Missing Expected Email Notifications ... 11
Cannot See my Secrets from the Platform as Cloudadmin ... 12
Cannot See a New Platform Group User in Secret Server ... 12

Cannot See Secret Server AD Groups or Users in Secret Server ... 13
Forgotten Username ... 13
Forgotten Password ... 13
Forgotten Cloudadmin Password ... 14
Persistent Login Issues ... 14
Regional Hosting Availability ... 14
Platform Architecture and Topology ... 14
Delinea Platform: High-Level Overview ... 15
Remote Access Service ... 17
Delinea Connector ... 17
Notification Services ... 19
Supported Browsers ... 19

Secret Server Integration ... 20

Current Secret Server Customers ... 20
New Delinea Customers ... 20
Opt-in to Platform Tenant via Secret Server Cloud ... 20
Automated Platform and Secret Server Cloud Integration ... 20
New Delinea Customers ... 20
Current Secret Server Customers ... 21
Logging in and Getting Started ... 25
Manually Integrate Secret Server Cloud ... 26
Retrieve the Platform Integration Credentials ... 27
Enable Platform Integration in Secret Server ... 27
Verify the Integration in the Platform ... 29
Verify the Integration in Secret Server ... 29
Manually Integrate Secret Server On-Premise ... 30
Accessing the Delinea Platform ... 30
Prerequisites ... 31
Integration Steps ... 31
Install a Remote Access Service Engine ... 31
Add a New Secret Server Connection ... 31
Update the Platform Integration Settings On Secret Server ... 33
Update Your Secret Server Connection with the RAS Site ... 33
Verify the Overall Integration ... 34

Delinea Connector ... 34

Determining whether you need the Delinea Connector ... 34
Installing the Delinea Connector ... 35
Requirements ... 35
Permissions Required for Alternate Accounts and Organizational Units ... 35
Set Read Access Permission to the User Account Container or Organizational Unit ... 36
Downloading the connector and getting a registration code ... 36
Installing and configuring the connector ... 37
Enabling auto-update for the connector ... 40

Updating the connector ... 41
Checking connector status ... 42
Connector Best Practices ... 43
Supporting user authentication for multiple domains ... 43
Configuring authentication for trusted domains ... 43
Configuring authentication for multiple forests without trust ... 45
Connector redundancy ... 46
Installing additional connectors ... 46
Additional information ... 46
Troubleshooting the Connector ... 46
Issue: While installing the Connector, I get this error message:The remote certificate is invalid according to the validation procedure. ... 46
Issue: While installing the Connector, I get this error message:Failed to obtain certificate or certificate verification failed. ... 47
Issue: While registering the Connector, I get this error message:Encountered unhandled exception in registering the proxy: System.ServiceModel.EndpointNotFoundException: There was no endpoint listening at http://<tenant url>/transport_rpc.svc ... 47
Issue: While registering the Connector during certificate checks validation, I get this error:(500) Internal Server Error ... 47
Issue: While registering the Connector, I get this error message:Failed to connect to server using REST RPC ... 48
Issue: After starting the Connector Configuration application, nothing happens for several minutes and the application is not accessible. ... 48
Issue: The Connector fails to connect to the platform. ... 49
Issue: Auto-update isn't working for my Connector ... 49
Issue: The Connector is correctly installed and active, but AD users can't log in and they get this error message: Authentication (login or challenge) has failed. Please try again or contact your system administrator. ... 49
Issue: I don't know where to access the Connector logs. ... 49
Issue: I don't know the default log rotation setting for the Connector logs ... 49
Issue: I want to use both Federation and Active Directory (AD) with the platform, but I don't know the best practices for doing this. ... 49
Issue: I can't query Active Directory users or groups from the platform, despite having an active connector. ... 50

Federation ... 50

Platform Federation Integrations ... 50
SP-Initiated vs IdP-Initiated SSO ... 50
SP-Initiated SSO ... 51
IDP-Initiated SSO ... 51
Federation Management ... 52
Add a Federation Service Provider ... 52
Enable a Federation Service Provider ... 53
Delete a Federation Service Provider ... 53
Advanced Settings (SAML only) ... 53

Re-authentication with the IdP 54
Prompt for Re-authentication (OIDC only) 54
Attribute Mappings 54
Group Mappings 55
User Mappings 56
Debugging Federation Setups 57
Analyzing Captured Logs 58
OIDC Flows 59
Integrating Auth0 60
Build an Auth0 SAML Application 60
Add the Provider to the Platform 62
Settings 65
Advanced Settings 65
Attribute Mappings 65
Adding Custom Claims 65
Group Mappings 66
User Mappings 66
Domains 66
Build an Auth0 OIDC Application 66
Add the Provider to the Platform 67
Settings 70
Attribute Mappings 70
Group Mappings 70
User Mappings 70
Domains 70
Integrating Microsoft Entra ID 70
Build an Entra SAML Application 70
Attributes and Claims Mappings 74
Add the Provider to the Platform 77
Settings 80
Advanced Settings 80
Attribute Mappings 81
Group Mappings 81
User Mappings 81
Domains 81
Build an Entra OIDC Application 82
Add the Provider to the Platform 85
Settings 89
Attribute Mappings 90
Group Mappings 90
User Mappings 91
Domains 91
Add the Platform 91
From Your Entra Application 92

From the Platform ... 93
Integrating Entrust ... 94
Build an Entrust SAML Application ... 94
Add a Delinea Platform SAML Provider ... 98
Build an Entrust OIDC Application ... 100
Add a Delinea Platform OIDC Provider ... 105
Test Configuration ... 107
Known limitation(s) ... 107
Integrating Okta ... 107
Build an Okta SAML Application ... 108
Add the Provider to the Platform ... 112
Settings ... 115
Advanced Settings ... 115
Attribute Mappings ... 115
Group Mappings ... 116
User Mappings ... 116
Domains ... 116
Build an Okta OIDC Application ... 116
Add the Provider to the Platform ... 117
Attribute Mappings ... 119
Group Mappings ... 119
User Mappings ... 120
Domains ... 120
Integrating OneLogin ... 121
Build a OneLogin SAML Application ... 121
Add a Delinea Platform SAML Provider ... 125
Build a Onelogin OIDC Application ... 127
Add a Delinea Platform OIDC Provider ... 130
Test Configuration ... 132
Known limitations ... 132
Integrating Ping Identity ... 132
Prerequisites ... 133
Build a Ping Identity SAML Application ... 133
Add the Provider to the Platform ... 134
Settings ... 136
Advanced Settings ... 136
Attribute Mappings ... 137
Group Mappings ... 137
User Mappings ... 137
Domains ... 137
Post-configuration to Ping Identity Application ... 137
Update Entity ID ... 137
Attribute Mappings ... 137
Activate the Application ... 138

Map Ping Identity and Platform Groups 139
From Your Ping Identity Application 139
From the Platform 140
Test Connection 140
Troubleshooting 141
Build a Ping Identity OIDC Application 143
Configure the Application on Ping Identity 144
Add the Provider to the Platform 144
Settings 146
Attribute Mappings 146
Group Mappings 146
User Mappings 146
Domains 147
Post-configuration to Ping Identity 147
Update Redirect URIs 147
Attribute Mappings 147
Enabling the Application 148
Test Connection 148

Multi-factor Authentication 149

About MFA 149
Identity MFA Profiles 150
View Authentication Profiles 150
Add a New Authentication Profile 150
Authentication Challenges 152
Global Security Settings 153
Security Questions 153
Security Devices 154
Identity Policies 155
Create and Assign an Identity Policy 155
Update an Identity Policy 156
Authentication 157
Services 158
Authentication Rules 158
Browser Session Parameters 159
Delinea Mobile Application Session Parameters 160
Other Settings 160
User Security 162
Self Service 162
Password Settings 164
OATH OTP 167
RADIUS 167
User Account Settings 167
Authentication Settings 168
Summary 170

MFA for Secrets ... 170
Availability ... 170
Default MFA Profile ... 171
Assigning MFA to Secrets ... 171
Assign MFA to an Individual Secret ... 171
Assign MFA to a Secret Policy ... 171
Assign MFA to Secrets through a Bulk Operation ... 172
Applying an MFA Profile to All Enabled Secrets ... 172
Considerations for Assigning MFA to Secrets ... 173
Corporate IP Range ... 173
Add an IP Range ... 174
Edit an IP Range ... 174
Delete an IP Range ... 174
RADIUS Configuration ... 174
Radius Authentication Overview ... 174
Configuring a RADIUS Server ... 174
Configuring the Delinea Connector as a RADIUS client ... 176
Using Multiple Delinea Connectors as RADIUS clients ... 177
Configure a RADIUS Authentication Profile ... 177
Configure a RADIUS Identity Policy ... 178
Using RADIUS Authentication ... 179
IWA Configuration ... 180
Prerequisites ... 180
Enabling IWA Service on the Connector ... 181
Importing a Certificate ... 181
Verifying IWA Over HTTPS ... 182
Enabling IWA in the Authentication Policy ... 183
Using IWA with Identity Cookie ... 183
Using IWA to Authenticate Application Access ... 184
Disabling IWA ... 184

Mobile Access ... 184

Administrators ... 185
Users ... 185
Platform Notifications ... 185

User Management ... 185

Avoid Adding Local Users ... 186
Adding Users ... 186
Adding a Local User Account ... 186
To Add a New Local User ... 187
Bulk Import Local User Accounts ... 188
Granting Access to User Accounts From External Directories ... 192
Adding Active Directory User Accounts ... 192
Adding Federated User Accounts ... 192

Managing Users ... 192
Overview ... 192
199
Groups ... 199
Roles ... 200
MFA Redirection ... 200
Additional Attributes ... 201
Activity ... 202
Policy Summary ... 203
User Profile ... 204
Group Management ... 209
Manually Synchronize New Platform and Secret Server Groups ... 209
Group Mappings ... 210
Enabled Platform Groups ... 210
Linking and Synching Groups ... 210
Assigning Secret Server Permissions to Platform Users ... 211
Automatically Create Groups During Synchronization ... 212
Predefined Groups ... 212
Adding a Group ... 213
Adding Users to a Group ... 213
User Directory Service Configuration ... 215
Additional Attributes ... 216

Roles and Permissions ... 217

Unified Roles and Permissions in Secret Server and Platform ... 217
Built-in Roles ... 217
Custom Roles ... 218
Permissions ... 218
Users, Groups, Roles, and Permissions ... 218
Edit Role Permissions ... 218
Edit Role Members (Groups) ... 220
Delete a Role ... 222
Assign a Group to a Role ... 222
Create a New Role ... 223
Add Members (Groups) to a Role ... 224
Platform Permissions ... 225

Delinea Engine Management ... 252

Engine Management Components ... 252
Engine Management Architecture ... 253
Engine System Requirements ... 254
Engine Security ... 256
Engine States ... 256
Engine Management Account Permissions and Roles ... 256
Network Communication ... 258

Protocols ... 259
About Delinea Engine Sites ... 259
About Delinea Engines ... 259
Managing Engine Sites ... 260
Create a Site ... 260
Edit a Site ... 260
Delete a Site ... 260
Managing Engines ... 261
Add an Engine ... 261
Automatically Update an Engine ... 263
Manually Update an Engine ... 263
Uninstall an Engine from the Platform ... 264
Manually Uninstall an Engine from Host Machine ... 264
Engine and Log Directories ... 265
Engine Logs ... 266
Adjust Engine Log Levels ... 267
Workloads ... 267
Workload Deployment States ... 267
Monitor Workloads ... 268
Delinea Audit Collector Workload ... 269
Edit Audit Collector Settings ... 269
Command Relay Workload ... 269
Command Relay Prerequisites ... 270
Edit Command Relay Settings ... 270
Command Relay Account Permissions ... 271
The DelineaZone ... 274
Minimal Permissions to Join a Server to a Zone ... 274
On Windows ... 274
On *nix ... 275
Engine Troubleshooting Guide ... 275
Issue: Engine does not appear, is outdated, or status shows “failed” ... 275
Issue: Engine upgrade problems ... 275
Issue: Need to manually reinstall engine ... 276
Issue: Workload status shows “failed” ... 276
Issue: Selected secret (domain admin account) for Command Relay stopped working ... 276
Issue: Getting 400s when engine is trying to register ... 276
Appendix: Engine and logs directory structure ... 277

Inventory ... 278

Viewing Your Platform Inventory ... 278
Launching into a Computer Asset ... 279
Launch (Login) Options ... 279
Launch with Manual Credentials ... 279
Launch with Use My Account ... 279
Launch with Secret ... 279

Disabling Inventory 280
PCS Policies 280
Using Secrets 280
Secret Server Overview 280
Secret Server Documentation for New Users 280
Secret Server Key Features 281
Secret Server Secrets 281
Secrets 281
Secret Folders 281
Checking out Secrets 282
Credential Management 282
Discovery 282
Distributed Engines 282
Remote Password Changing 283
Auditing Privileged Account Activity 283
Advanced Session Recording and Management 283
Audit Logs 284
Alerts 284
Built-in Reports 284
Remote Access Service 284
Setting Up RAS 285
RAS Requirements 285
Useful Tools 286
Sizing Guidance for RAS Engine Linux Hosts 286
Set Up a RAS Engines Site 287
Naming a RAS Site 288
Renaming RAS Site 289
Install RAS Engines 291
Engine Rules 291
Installing the Remote Access Engine 291
Installer Script Rules 293
Run the Installation Script 293
Configuring the RAS Engine to Use a Proxy Server (Optional) 293
Activate RAS Engines 295
Add Secret Templates to RAS 296
Secret Server Cloud 296
Secret Server On Premises 296
Uninstall RAS Engines 297
Automated Uninstallation 297
Manual Uninstallation 298
Using RAS 299
RAS Sites 299
Naming a RAS Site 299

Launch a RAS Session ... 300
From Secret Server On Premises ... 301
Update RAS Engines ... 302
Updating a RAS Engine ... 302
Manually Updating a RAS Engine ... 304
Using the Delinea Menu ... 305
Transfer Files ... 306
Session Information ... 306
Settings ... 306
Screenshot ... 307
Clipboard ... 307
Enter Full Screen ... 308
Disconnect ... 309
Transfer Files With RAS ... 309
Prerequisites ... 309
Download a File ... 309
Upload Files ... 311
Queue Tab ... 312
Current Limitations ... 314
Remote Access Permissions and Roles ... 315
RAS Engine Host Hardening ... 318
General Hardening Steps ... 319
Restrict Incoming Port Access to All RAS Engine Servers ... 319
Remove Unnecessary User Groups ... 319
Rename Default Accounts ... 319
Disable Services ... 319
Restrict Network Protocols ... 319
SSL/TLS Settings ... 319
System Admin (Universal) ... 320
Network SSH/OpenSSL: ... 320
Auditing ... 320
CIS standards ... 321
Ubuntu ... 322
System Ubuntu: ... 322
Directories, Files and Permissions ... 323
Red Hat Enterprise Linux (RHEL) ... 323
System RHEL: ... 323
Directories, Files and Permissions: ... 324
Network SSH/OpenSSL: ... 324
Entitlements and Licenses ... 324
RAS Troubleshooting ... 325
Failed to Connect to the Target Machine. Error Showing When Attempting to Launch a Remote Session ... 325
RDP Supported Authentication Methods ... 325
The Engine is Configured Properly But a Connection to the Target Cannot Be Established ... 326

Accessing Logs on the Target Server 326
The Engine Shows as "Offline" in the Sites and Engines UI 327
Unable to Open an SSH Session From the Web UI 328
Unable to Open an RDP Session From the Web UI 328
Engine Seems to be Functioning in an Unexpected Manner 329
Setting a Static UUID in Skytap 329
Issues Encountered While Installing the RAS Engine 331
Warnings That Can Occur During Installation: 331
Errors That Can Occur During Installation: 332
Uninstallation of the RAS Engine is Not Working From the Web UI. 333
Start/Stop Commands 333
Unable to Launch SSH Sessions via Secret Server Distributed Engine 334
Issues Connecting to On-Prem Secret Server 335

Insights 335

Audit 335
Behavioral Analytics 336
Audit 336
Reviewing Sessions 336
Enabling Session Review 336
Viewing Sessions 338
Using Video Features 342
Analyzing a Recording 342
Sharing Sessions 344
Viewing Audit Logs 344
Accessing Audit Logs 345
Viewing The Audit Log 345
Downloading Data 346
Secret Server Services 347
Audit Collector Services 354
Permissions Services 368
Identity Federation 368
Policy 369
Certificate Management Services 370
Identity Services 370
RAS Services 372
Registration Services 373
Behavioral Analytics 374
Risk Based Behavioral Analytics 374
High Level Architecture 374
Behavioral Analytics Requirements 374
Behavioral Analytics Setup 375
Integrate Behavioral Analytics into Secret Server 375
Import Historical Data from Secret Server 377
Using Behavioral Analytics 378

Alerts Page ... 379
Alert Details View ... 382
Users Page ... 385
Secrets ... 386
IP Addresses ... 387
Behavioral Analytics Customization ... 389
Alert Settings ... 389
Secret Server Integration Settings ... 391
Roles Settings ... 392

Marketplace ... 393

Applications and Tools ... 393
Integrations ... 395
Download Center ... 396

Webhooks ... 397

Current Capabilities ... 397
Delinea Platform SIEM Integrations ... 397
Webhooks Management ... 397
Creating a webhook ... 397
Testing a Webhook ... 398
Managing a Webhook ... 400
Integrating Azure Sentinel ... 400
Prerequisites ... 401
Configuring Azure Sentinel ... 401
Creating a Logic App in Azure ... 401
Setting up Azure Log Analytics ... 402
Integrating Webhooks and Azure Sentinel ... 405
Verifying Logs for the Azure Sentinel Webhook ... 406
Integrating Splunk Enterprise ... 407
Prerequisites ... 407
Setting up Splunk Enterprise ... 407
Creating a Certificate in Zero SSL ... 408
Configuring a Certificate in OpenSSL ... 409
Integrating Webhooks and Splunk Enterprise ... 411
Configuring Splunk Enterprise HTTP Event Collector ... 411
Creating Webhooks for Splunk Enterprise ... 415
Verifying Logs for Splunk Webhook ... 416

Managing Third-Party Contractors and Vendors ... 417

Local Users ... 418
Bulk Import of Vendors ... 418
Federated Vendors ... 418

Privilege Control for Servers ... 419

The Privilege Control Agent ... 419

PCS Policies ... 419
Inventory ... 419
Engine Management ... 419
Audit Collector ... 420
Command Relay ... 420
PCS End-to-End Installation and Run Guide ... 420
Assumptions ... 420
Overview ... 420
Configuring Firewall Ports for PCS ... 421
Setting Up PCS Service Accounts ... 421
Installing the Delinea Connector on Managed Servers ... 421
Enable IWA Service on Connectors ... 422
Allowing IWA Connections for All Users in the Default Policy ... 422
Obtaining an IWA Connector Host Certificate ... 423
Download the Connector Host Certificate ... 425
Distribute the Connector Host Certificate for Agent Installation ... 426
Installing the Delinea Engine on Managed Servers ... 430
Updating the Engine Management Settings ... 431
Update the Engine ... 431
Installing the Delinea Agent on Managed Servers ... 432
Download the Agent ... 432
Install the Linux Agent ... 433
Upgrade the Linux Agent ... 433
Install the Windows Agent ... 434
Setting up PCS Profiles ... 436
Emergency Access Profiles ... 436
Endpoint Login Profiles ... 437
Privilege Elevation Profiles ... 437
Setting up PCS Policies ... 437
View Policies ... 437
Deployment Status ... 437
Create a Policy ... 437
Policy Details ... 439
Policy Subjects ... 439
Policy Targets ... 440
Policy Conditions ... 440
Policy Rules ... 440
Setting up Audit and Session Recording ... 441
Viewing Audit Session Recordings ... 441
Setting up Use My Account for *nix Systems ... 442
Setup Using Delinea OpenSSH ... 442
Using OS Stock Version of OpenSSH ... 442
Automatic Script for UMA ... 442
Manual Steps ... 443

Testing Use My Account ... 444
Agents Reference ... 445
Installing Agents on Computers to be Managed ... 445
About the Deployment Process ... 446
Select a Target Set of Computers ... 446
Options for deploying Privilege Control Agent Packages ... 446
Install Silently Using a Configuration File ... 447
About the Sample Configuration Files Available ... 448
Setting the Parameters in a Custom Configuration File for the Installation Script ... 448
Customizing the Return Codes for the Installation Script ... 452
Use Other Automated Software Distribution Utilities ... 453
About the Files and Directories Installed on the Agent ... 453
Joining an Active Directory Domain at a Later Time ... 454
PCS Troubleshooting Guide ... 455
Issue: I don't know where to find all my log files. ... 455
Delinea Connector ... 455
Delinea Engine ... 455
Command Relay ... 455
Privilege Control Agent ... 455
Issue: Windows Diagnostics Error for MFA ... 455
Issue: How do I upgrade the Agent? ... 456
Policies ... 457
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. ... 457
Issue: My Policy is stuck on “Activating” (or “Deactivating”) status? ... 457
Issue: My Policy status is “Active” but it's not being enforced. ... 457
Issue: My Login (or Elevation) Policy status is “Inactive” but I can still perform Login (or Elevation) on the machine. Why? ... 457
Issue: The Policy’s Target list is not showing the machine I want to select. ... 457
Command Relay / Delinea Engine ... 457
Issue: How do I turn on debugging for my Engine? ... 458
Issue: Is Delinea Command Relay setting in Engine Pool for all engines under the same site? ... 458
Issue: Why does Command Relay need the Active Directory domain admin credentials? ... 458
Issue: What happens if I provide the wrong Active Directory domain admin credentials or if they expire? ... 458
Issue: My selected secret for Command Relay stopped working (domain admin account) ... 459
Issue: Command Relay can't log in using the same secret that works for Secret Server Discovery service? ... 459
Secret Server ... 459
Issue: My Secret Server Distributed Engine is not working. ... 459
Privilege Control for Servers Agent ... 459
Issue: How do I turn on/off debugging for Linux agents? ... 459
Issue: How do I turn on debugging for the sshd server? ... 460
Issue: How do I collect debug info for the Delinea team to investigate an issue? ... 460
Issue: My AD forest has multiple domains, so will each domain have a DelineaZone created? ... 460

Issue: My AD user cannot log in to the domain-joined Linux machine 460
Issue: My AD user can't run DZDO commands in the domain-joined Linux machine 461
Issue: I need Some Useful Commands and Tips for AD Client on *.nix 462
Issue using DirectControl Authentication on *NIX systems 468
PCS Technical Reference 468
Storing Privilege Control Properties in Active Directory 468
Core Agent Components and Services 469
What Happens During the Typical Log-on Process 472
How Failover and Disconnected Access Work 474
Preparing to Use Multi-Factor Authentication 477
Authorizing Basic Access 477
Checking rights and roles with the dzinfo program 477
Testing Command Rights 478
Troubleshooting Authentication and Authorization 478
Diagnostic tools and log files 478
Logging to the circular in-memory buffer 479
Collecting Diagnostic Information 479
Working with Domain Controllers and DNS servers 480
Configuring the DNS Server Role on Windows 480
Configuring DNS Running on UNIX Servers 480
Setting up DNS Service on a Target Domain Controller 481
Configuring UNIX to use DNS service on the target domain controller 481
Setting the domain controller in the configuration file 482
Using the fixdns script 482
What the Privilege Control DNS Subsystem Provides 483
Resolving a host name or IP address 483
Selecting a DNS server 484
Specifying DNS-related parameters 484
Filtering the objects displayed 484
Using Use My Account 485
Installing Agents on Computers to be Managed 485
About the Deployment Process 486
Select a Target Set of Computers 486
Options for deploying Privilege Control Agent Packages 486
Install Silently Using a Configuration File 487
About the Sample Configuration Files Available 488
Setting the Parameters in a Custom Configuration File for the Installation Script 488
Customizing the Return Codes for the Installation Script 492
Use Other Automated Software Distribution Utilities 493
About the Files And Directories Installed on the Agent 493
Joining an Active Directory Domain at a Later Time 494
Identity Threat Protection and Privilege Control for Cloud Entitlements 495
Identity Threat Protection 495
Privilege Control for Cloud Entitlements (PCCE) 495

Setting Up ITP/PCCE ... 495
Inventories ... 496
Inventory Types ... 496
Inventories User Interface ... 497
Filter the inventory table ... 497
Search by custom properties ... 499
Sort the inventory table ... 499
Other views ... 499
Configure table columns ... 500
Export the table as CSV ... 500
Use tags ... 500
Inventory Filter Properties ... 502
Identities ... 502
Groups ... 513
Assets ... 514
Memberships ... 515
Access Policies ... 515
Privileges ... 521
Activities ... 521
Identities ... 524
Filter and modify the table display ... 524
Insight into selected table data ... 525
Insight into selected filter options ... 525
Groups ... 525
Filter and modify the table display ... 525
Insight into selected table data ... 526
Assets ... 526
The Assets Page ... 526
Insight into selected table data ... 527
Memberships ... 527
Filter and modify the table display ... 527
Insight into selected filter options ... 528
Access Policies ... 528
Filter and modify the table display ... 528
Privileges ... 529
Filter and modify the table display ... 529
Insight into selected filter options ... 529
Activities ... 530
Filter and modify the table display ... 530
Dynamic Scopes ... 530
System Scopes ... 530
Custom Scopes ... 534
Access Explorer ... 534
Direct vs. Indirect Access ... 535

Recurring Reports 538
Identity Posture 538
Onboarding Process 539
Best Practices 539
Apps Overview 539
Checks 540
Onboarding Process 540
Best Practices 540
The Checks side panel 541
Shadow Admins 542
Actions 542
Azure Permissions 544
Threat Center 546
Detection Rules 546
The Detection Rules Table 546
Automated Response 550
Incidents 551
The Incidents page 551
The Incidents Pane 553
Risk Configuration 553
Risk types 554
Configure Risk 554

Branding 555

Preview Program 557

Opt-in 557
Opt-out 557
Feedback 558
Public Preview Features 558

Primary Navigation 558

Primary Left Navigation Menu 558
Secondary Navigation 559
Hover over a menu item 559
Click a menu item 561

Release Notes 562

Platform Change Log 563
Overview 563
Thursday, May 16, 2024 563
Friday, May 10, 2024 563
Friday, May 3, 2024 563
Monday, April 15, 2024 564
Friday, April 12, 2024 564
Tuesday, April 2, 2024 564

Thursday, March 28, 2024 ... 564
Wednesday, March 27, 2024 ... 565
Tuesday, March 22, 2024 ... 565
Wednesday, March 20, 2024 ... 565
Tuesday, March 19, 2024 ... 566
Tuesday, March 12, 2024 ... 566
Monday, March 11, 2024 ... 566
Friday, March 1, 2024 ... 567
Friday, February 23, 2024 ... 567
Wednesday, February 21, 2024 ... 568
Thursday, February 15, 2024 ... 568
Thursday, February 8, 2024 ... 568
Wednesday, January 24, 2024 ... 569
Thursday, December 14, 2023 ... 569
Tuesday, November 28, 2023 ... 570
Monday, November 20, 2023 ... 570
Tuesday, November 7, 2023 ... 570
Wednesday, November 1, 2023 ... 570
Tuesday, October 31, 2023 ... 570
Wednesday, October 25, 2023 ... 571
Tuesday, October 24, 2023 ... 571
Wednesday, October 11, 2023 ... 572
Tuesday, October 3, 2023 ... 572
Tuesday, September 26, 2023 ... 572
Friday, September 15, 2023 ... 573
Tuesday, September 12, 2023 ... 573
Thursday, August 3, 2023 ... 573
Friday, July 28, 2023 ... 574
Thursday, July 27, 2023 ... 574
Friday, July 21, 2023 ... 574
Wednesday, July 5, 2023 ... 575
Wednesday, June 28, 2023 ... 575
Wednesday, June 14, 2023 ... 575
Wednesday, June 7, 2023 ... 575
Wednesday, May 10, 2023 ... 575
Monday, April 17, 2023 ... 576
Monday, April 10, 2023 ... 577
Wednesday, March 29, 2023 ... 577
Friday, March 17, 2023 ... 577
Wednesday, March 15, 2023 ... 577
Spring (Q2) 2024 Release ... 578
Secret Server on Platform ... 578
Remote Access Service (RAS) ... 578
Connection Manager (CM) ... 578

Inventory 578
Audit 579
Marketplace & Integrations 579
Identity & Federation 580
Engine Management 580
Privilege Control for Servers 580
Delinea Mobile App 580
Web Password Filler (WPF) 580
Other updates 580
Winter (Q1) 2024 Release 581
Secret Server on Platform 581
Remote Access Service (RAS) 581
Connection Manager (CM) 581
Audit 582
Marketplace & Integrations 582
Identity & Federation 582
Other updates 582
Fall (Q4) 2023 Release 582
Secret Server on Platform 582
Remote Access Service (RAS) 582
Web Password Filler (WPF) 583
Connection Manager (CM) 583
Marketplace & Integrations 583
Identity & Federation 583
Other updates 584
Summer (Q3) 2023 Release 584
Secret Server on Platform 584
Remote Access Service (RAS) 584
Web Password Filler (WPF) 584
Connection Manager (CM) 584
Audit 584
Marketplace & Integrations 585
Identity & Federation 585
Other updates 586
Spring (Q2) 2023 Release 586
New Hosting Regions 586
Behavioral Analytics (Private Preview) 586
Permissions Service 586
Improved Home Screen 587
Marketplace 587
Tenant Customization 587
Winter (Q1) 2023 Release 587
Seamless Integration with Secret Server Cloud 587
Next-Gen Remote Access Service 587

Robust Identity and Federation Services 588
Marketplace 588
Foundational Shared Services 588
SMS Terms of Service 589

Welcome to the Delinea Platform

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.

Navigation

You can navigate the full set of platform documentation using the section links on the left. If a section has sub-sections, links to the sub-sections will appear beneath the section link when you click the down arrow. Most top-level section pages provide significant information on their own, but some contain minimal text, with links to sub-sections that provide the actual instructions. You can navigate content on an individual page using the links on the right. You can also enter search terms in the search field at the top of any page.

Introduction to 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.
- **Cloud-Native**: Experience the most resilient solution, boasting 99.99% uptime.

Learn more about Delinea Platform and its shared service capabilities.

Features

Secret Server

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

Remote Access Service

- 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.
- 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.

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.

Robust Identity and Federation Services

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

Built-in Delinea Marketplace

The Delinea 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.

To begin using the platform, proceed to the next section, "Getting Started" below

Getting Started

This Getting Started guide should help you to get up and running on the Delinea Platform fairly quickly. The Overview provides a list of the tasks covered as well as general tips including the purpose of the first two accounts: cloudadmin and Platform Admin.

To troubleshoot common platform onboarding issues, see Onboarding Troubleshooting.

Overview

The Getting Started guide provides initial instructions for the tasks below. Links to the full procedures are provided where relevant in each section. Steps 1, 2, and 3 must be completed in order, before completing the other tasks. Steps 4, 5, and 6 must also be completed in order.

1. Provision and Log into the platform
2. Add Domain User Accounts
3. Assign Yourself Admin Permissions and Access Secrets
4. Link platform and Secret Server Groups
5. Synch platform and Secret Server Groups
6. Assign Secret Server Permissions to platform Users

- Automatically Create Groups During Synchronization
- Set Up and Use Remote Access Service
- Assign Roles and Permissions to Users and Groups

General Tips

The Cloudadmin Account

As the first person to set up the Delinea Platform, **cloudadmin** is the first account you will need to perform initial platform provisioning, login, integration, and setup tasks, including authorizing domain user accounts on the platform, and setting up a second platform Admin account for yourself based on a domain account of your own. Cloudadmin is a local platform account created for you, in the format `cloudadmin@yourplatformtenantname`.

Note for existing Secret Server customers only: Because cloudadmin is not your Secret Server admin 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 admin 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 platform and Secret Server.

Your Platform Admin Account

To gain Secret Server admin permissions and see secrets *from the platform*, you must do the following while logged in as cloudadmin:

Step 2 below: Add Domain User Accounts to the platform, including one of your own personal domain user accounts.

Step 3 below: Assign Yourself Admin Permissions and Access Secrets to creating a **Platform Admin** account for yourself based on your personal authorized domain user account.

Note: Both the cloudadmin and Platform Admin accounts initially have comprehensive administrator permissions on the platform. For cloudadmin, we recommend leaving the comprehensive permissions unless you have a clear and logical plan for distributing some of them to other administrator accounts. For Platform Admin, we recommend removing permissions that are not required for carrying out day-to-day platform administration tasks as soon as possible. We also recommend creating multiple administrator roles, each with a different set of permissions for specific purposes.

1. Provision and Log into the Platform

Procedures for provisioning and logging into the platform are presented for three user groups:

- Current Secret Server Cloud Customers Opting into the platform
- New or Prospective Delinea Customers
- Current Secret Server On-Premise Customers

For Current Secret Server Cloud Customers

Current Secret Server Cloud customers with specific permissions and entitlements can opt into the platform through their Secret Server Cloud instance, following the basic procedure below:

1. Log into your Secret Server Cloud instance as a Secret Server tenant administrator with platform integration permissions.
2. Near the top of the portal, click the **New!** button.
3. In the window that opens, follow the on-screen instructions to provision your new platform tenant, set up platform integration with your Secret Server Cloud instance, and log into the platform.

For complete instructions, see Opt-in to Platform Tenant via Secret Server Cloud.

Note: When a Secret Server administrator clicks the button to Opt-in to Delinea Platform integration, their Secret Server users will not have immediate access to the platform until the administrator sets up SSO, federation, and AD sync on the platform. For more information, see The Delinea Connector, Federation, and Integrating Microsoft Entra ID.

For New or Prospective Delinea Customers

New or prospective Delinea customers can purchase or sign up for a trial of a Delinea Platform tenant with built-in, integrated Secret Server/Secret Server functionality by taking the steps below.

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 into the Delinea Support portal:
   - 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.

For Current Secret Server On-Premise Customers

Current Secret Server On-Premise customers can access Remote Access Service through the Delinea Platform by contacting by contacting a Delinea sales representative to request a Delinea Platform tenant without Secret Server Cloud.

2. Add Domain User Accounts

On the Delinea Platform, domain (non-local) groups are *mapped, not added* to named platform identity groups. You can authorize domain user accounts on the platform by using the Delinea Connector for Active Directory users, or by using Federation (IdP) for federated users.

Connector is required only for AD users, so if you're going to have only AD users on the platform, you need to set up the connector but you don't need federation.

Federation is required only for federated users, so if you're going to have only federated users on the platform, you need to set up federation but you don't need the connector.

If you're going to have both AD and federated users on the platform, you'll need to use the connector and federation.

Note: Users should be added to the platform only through federation or through their membership in an Active Directory. Adding local users to the platform is not considered a best practice for privileged access management, for the reasons explained **here**.

2a. Add Active Directory User Accounts

To add Active Directory user accounts to the platform, you must use the Delinea directory Connector. For complete instructions on downloading, installing, and registering the Connector, see The 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 a domain where you have a personal account.

To map Microsoft Entra ID groups to platform groups, see Integrating Microsoft Entra ID.

2b. 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 into 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.

Local User Acounts

Users should be added to the platform only through federation or through their membership in an Active Directory. Local user accounts should be used ***very rarely***. 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. Adding local users to the platform is not considered a best practice for privileged access management, for the reasons explained in User Management.

Note: Local accounts cannot be converted to domain accounts.

Note: After the Connector is installed and Active Directory is set up on the platform, do not add an existing SSC 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.

3. Assign Yourself Admin Permissions and Access Secrets

After you have authorized domain 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.

3a. Assign Platform Admin Permissions to Your Personal Domain Account

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.

3b. Assign Secret Server Admin Permissions to Your Personal Domain Account

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 synched 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 synched Secret Server group.

3c. Access Secrets from the Platform

After you have assigned platform and Secret Server administrator permissions to your personal AD account, you can access Secrets from the platform.

1. Log out of the platform as Cloudadmin.
2. Log back into the platform using your Platform Admin 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.

Link Platform and Secret Server Groups

Note: For new platform customers who weren't using Secret Server previously, platform groups and Secret Server groups no longer need to be linked and synchronized. For example, when a user opens a secret, clicks the Sharing tab, and searches for groups, Secret Server and platform groups are both queried simultaneously. Those users can skip this section.

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.

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.

For detailed instructions on synchronizing platform and Secret Server groups, see Group Management.

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*.

Sync 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.

Assign Secret Server Permissions to Platform Users

Platform permissions are unrelated to Secret Server permissions. But platform users need Secret Server permissions to access their secrets and Secret Server admin privileges. Secret Server permissions can be assigned to platform users by linking a platform to an Enabled Platform Group in Secret Server, then assigning Secret Server permissions to the platform accounts in the linked Secret Server group.

1. Click **Secret Server** from the left navigation menu.
2. Click **Access** from the left navigation, then select **Groups**.
3. Click to open an Enabled Platform Group.
4. Click the **Roles** tab.
5. Click **Assign to roles**. A list opens of all available Secret Server roles (with attached permissions).
6. Check the box next to each role you wish to assign to the group.
7. Click **Save**.

For detailed instructions on assigning Secret Server permissions to platform users, see Group Management.

Automatically Create Groups During Synchronization

Instead of manually linking a Secret Server group to a platform group, you can choose to automatically create new Enabled Platform Groups in Secret Server during the periodic group synchs. When you enable the Create Groups During Synchronization feature, Secret Server checks all associated platform users to see if any belong to a platform group that is not yet linked to a Secret Server group. If an unlinked platform group is found, Secret Server automatically creates and links a corresponding Secret Server group to it.

1. Click **Settings** from the left navigation menu, then select **Administration** under Secret Server.
2. On the Secrets Administration page, click **Platform Integration**. The Platform Integration page opens to the Configuration tab.
3. Click **Edit** next to Platform Integration Configuration.
4. Scroll down and select the box next to **Create Groups During Synchronization**.
5. Consider the warning message that appears:

   Warning! Enabling "Create Groups During Synchronization" can create a large number of groups locally if the Platform users are members of many groups in Platform, including groups through external directory services such as Active Directory or Microsoft Entra ID federation.
6. Click **Cancel** to cancel, or click **Save** to automate the creation of new Enabled Platform Groups in Secret Server during the periodic group synchs.

Set Up and Use Remote Access Service

The Delinea Remote Access Service (RAS) 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 RAS engine, make sure you meet the minimum requirements. See RAS 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 RAS Session

To launch a RAS 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 RAS.
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 RAS connection to a remote machine.

For more detailed instructions on using the Remote Access Service, see Using RAS.

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 RAS 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.

Onboarding Troubleshooting

This page provides tips that should help you resolve potential issues when onboarding to the platform.

Finding Your Delinea Support PIN

To find your PIN to access Delinea Support services:

1. Make sure you have followed the original email instructions for logging into the Delinea Cloud portal and Support portal.
2. Log in to the Delinea Support Portal.
3. Click **Cloud Portal**.
4. Click **Thycotic One/Cloud Manager**.
5. Click **Generate Tech Support PIN**.
6. Click **Generate Privileged PIN**.
7. Click **OK**.

Missing Expected Email Notifications

After you are approved for a platform trial, you should receive the following sequence of three emails from Delinea during your on-boarding process, as described below:

1. ***Welcome to your Secret Server Cloud Trial on the Delinea Platform***
   - Sent after you are approved for a trial
   - Complete the tasks in this email to receive the second email
2. ***Welcome to the Delinea Support Portal!***
   - Sent after you complete tasks in email #1
   - Complete the tasks in this email to receive the third email
3. ***You have been invited to the <tenant-name> tenant on Delinea Platform***
   - Sent after you have logged into the Support portal
   - Note the provided cloudadmin account login/username and click **Accept Invitation**.
   - Although the invite link in the email is long-lived, it will expire and can only be used once.

If you are having issues receiving email notifications from the Delinea Platform, here are several things you can check to troubleshoot the issue:

1. Start by checking your spam or junk folder. Sometimes legitimate emails can be filtered as spam by mistake.
2. Review your email settings to see if you have any filters or rules set up that may be diverting or deleting incoming emails.
3. If your IT organization is using spam filtering services, check that these emails are not blocked by those solutions. If necessary, you can add the **delinea.app** domain to the appropriate **allowlist** rules.
4. If your mail server configuration requires the allow-listing of IP addresses to receive mail or to support STARTTLS, our mail server IP addresses are as follows:
   - 54.240.75.72
   - 54.240.75.73
   - 149.72.129.10
5. Make sure the email account you are searching through is the email account you used to sign up for the platform.
6. If you need additional information or require the email to be resent, contact Delinea Support.

Cannot See my Secrets from the Platform as Cloudadmin

While you are logged in as cloudadmin you will not have your existing Secret Server admin permissions and you will not be able to see your existing secrets in Secret Server. ***This is expected behavior and it does not indicate a failed integration***. To gain your existing Secret Server admin permissions and see your existing secrets *from the platform*, you must first set up active directory users and then assign platform and Secret Server admin permissions to your personal domain account as described in steps 2 and 3 in Getting Started.

Cannot See a New Platform Group User in Secret Server

When you add a user to a platform group that is synched to a Secret Server group, you might not see the user in the Secret Server group right away. The background process updates the Secret Server group members at set intervals. To speed the process:

1. Click **Settings** from the left navigation.
2. Click **Platform integration** on the Settings page.
3. On the Platform Integration page, select the **Groups** tab.
4. In the Enabled Platform Groups section, click **Sync Now**.

For instructions on synchronizing platform groups to new Secret Server groups, see Group Management.

Note: A new AD or Federated user will not appear on the platform until they log in for the first time.

Cannot See Secret Server AD Groups or Users in Secret Server

When you click **Access** from the left navigation then select **Users**, you might not see Active Directory users and groups that have been set up in Secret Server. To see these users and groups, two things must happen:

- A platform administrator must set up the Delinea directory Connector on the Platform and sync the SSC AD users/groups through the Group Sync function
- The SSC AD users must log into the platform at least once, to be automatically provisioned on the platform and logged into Secret Server from the platform

Forgotten Username

If you are trying to log in to the platform and you forgot your username:

1. In the **Username** field, try entering the email address associated with the account you're logging in with. If your email address is unique on the platform, you should be able to log in that way. If the same email address is used for multiple accounts on the platform, the login process gives precedence to a domain or federated user account first, before a local account.
2. To retrieve your forgotten username, click **Forgot username** in the login dialog.
3. When prompted, provide the email address for the account you're trying to log in with.
4. Look for an email from Delinea containing your username and a login link. If you've used the same email address for multiple platform accounts, the Delinea email will provide all usernames associated with that email.
5. Click the login link in the email and log in with your username from the email.

Forgotten Password

If you are trying to log in to the platform and you forgot your password:

1. Enter your username in the login dialog.
2. Click **Forgot password** in the subsequent dialog.
3. When prompted, respond to the multi-factor authentication (MFA) challenge.

   Note: depending on the rules applied to your authentication profile, this challenge could come through email, SMS, mobile application, or phone call.
4. Answer the MFA challenge correctly.

5. When prompted, reset your password.
6. Return to the login dialog and log in with your new password.

Forgotten Cloudadmin Password

If you are the cloudadmin and you forget your password:

1. Contact Delinea support staff, who will verify your identity and provide you with a one-time password (OTP).
2. Use the OTP to log in as cloudadmin.
3. After logging in, change your password when prompted.

Persistent Login Issues

If you know you have correctly entered your login username and password but still can't log into the platform:

Ask a platform administrator to verify that your account information is correct.

- If your account information is incorrect, use the correct information provided by your platform admin.
- If your information is correct, ask the platform administrator to check the licensing page (cloud subscription) in Secret Server for available user licenses and correct dates.

Regional Hosting Availability

The Delinea Platform has been growing rapidly, and we recognize the importance of having hosting infrastructure in key locations around the world to ensure fast and reliable access for all our customers. Because the Platform is hosted in Microsoft Azure, we can leverage the benefits of public cloud computing and quickly expand into new regions as new requirements demand it.

Below are the geo-locations and regions where the Delinea Platform is currently deployed.

Geography	Regional Pair A	Regional Pair B
Southeast Asia	East Asia (Hong Kong)	Southeast Asia (Singapore)
Europe	West Europe (Netherlands)	North Europe (Ireland)
Canada	Canada Central (Toronto)	Canada East (Quebec City)
Australia	Australia East (New South Wales)	Australia Southeast (Victoria)
UK	UK South (London)	UK West (Cardiff)
US	East US (Virginia)	East US 2 (Virginia)

Platform Architecture and Topology

The architectural diagrams provided in this article help you with a high-level understanding of the underlying infrastructure and technology stack that supports the Delinea Platform. Additionally, you can leverage this material if you are interested in allowing access to the Delinea Platform and its related services in your firewall.

We are continuously improving and optimizing our architecture to ensure that our service is scalable, secure, and efficient.

Note: The suggested list of ports in this document shows all of the default port numbers. These default ports may differ based on your environment and your own unique requirements. In all cases, the ports and addresses listed below should be excluded from packet inspection to allow for normal service operation.

Delinea Platform: High-Level Overview

- The diagram below highlights the overall architecture of the Delinea Platform.
  - Shared services are foundational services that provide infrastructure and other common resources that are designed to be consumed by various applications such as authentication, notification, and audit.
  - Application services are built on top of the platform shared services, and are designed to provide functionality that is unique to the application such as vaulting and remote access.

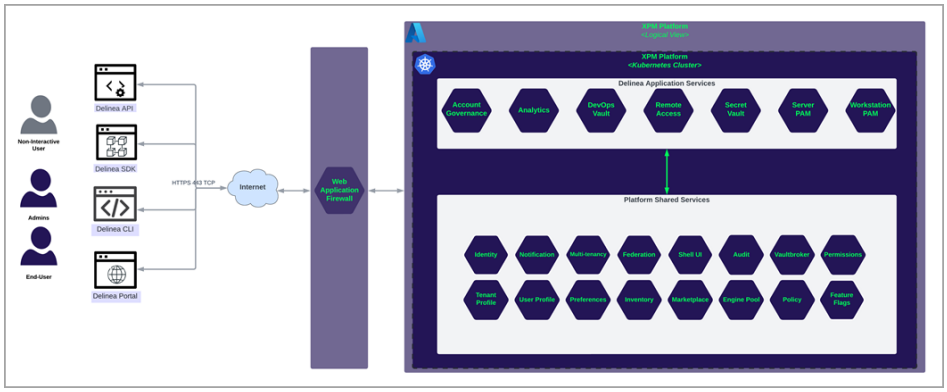
    Note: The Delinea Platform is evolving with every new release. The overview diagram below may be forward-looking from that perspective.
- Delinea Platform leverages Imperva Cloud Web Application Firewall to help secure our edge services. Customers who are interested in applying outbound filtering should be able to lock down their access to the *ingress Imperva* IPs according to Imperva Documentation.

Note: The IP ranges from Imperva may change periodically, and it is important to check frequently and stay up to date. IP ranges can be retrieved via the Imperva API as well - an example is below:

```
  curl -s --data "resp_format=json" https://my.imperva.com/api/integration/v1/ips | json_
pp
  {
   "debug_info" : {
      "id-info" : "999999"
   },
   "ipRanges" : [
      "199.83.128.0/21",
      "198.143.32.0/19",
      "149.126.72.0/21",
      "103.28.248.0/22",
      "185.11.124.0/22",
      "192.230.64.0/18",
      "45.64.64.0/22",
      "107.154.0.0/16",
      "45.60.0.0/16",
      "45.223.0.0/16",
      "131.125.128.0/17"
   ],
   "ipv6Ranges" : [
      "2a02:e980::/29"
   ],
   "res" : 0,
   "res_message" : "OK"
}
```

- Customers interested in implementing inbound filtering can restrict access to traffic originating from the Delinea Platform to the specified egress IP address ranges below:
  - 13.68.202.64/29
  - 74.235.247.24/29
  - 137.116.238.240/29
  - 108.143.39.32/29
  - 4.180.243.168/29
  - 23.100.88.32/29
  - 65.52.165.168/29
  - 104.215.150.80/29
  - 172.203.27.16/29
  - 23.101.212.8/29
  - 104.210.77.120/29
  - 20.11.207.32/29
  - 40.85.216.32/29
  - 40.85.241.48/29
  - 40.86.243.40/29
  - 20.90.1.200/29
  - 51.140.10.160/29
  - 51.145.8.56/29
- To obtain detailed information regarding the ingress and egress IP ranges used by Secret Server Cloud, please consult Secret Server Hybrid Multi-Tenant Cloud Architecture.

Delinea Platform: High-Level Overview

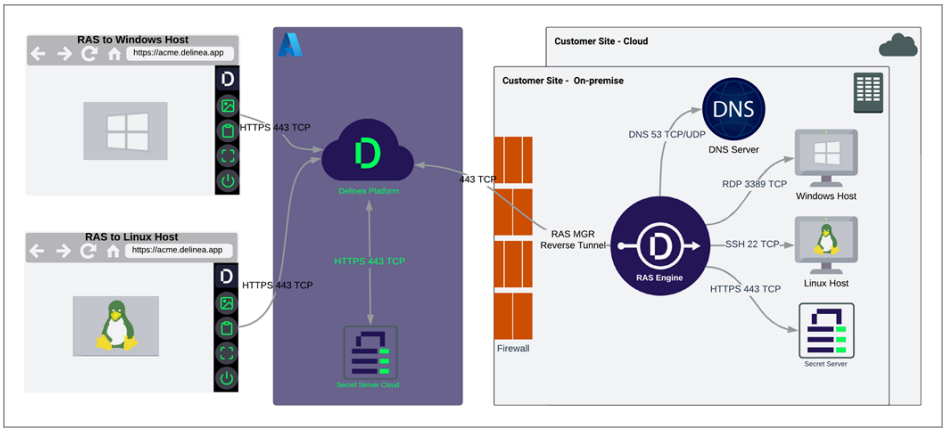


Remote Access Service

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

- No internet-facing ingress ports are required for the RAS Engine
- Outbound access on port 443 TCP from RAS Engine to the Delinea Platform via Imperva ingress
- Internal access on port 53 TCP/UDP from RAS Engine to DNS server for name resolution of target machines
- Internal access on port 3389 TCP from RAS Engine to Windows-based target machines for RDP access
- Internal access on port 22 TCP from RAS Engine to Linux-based target machines for SSH access
- Internal access on port 443 TCP from RAS Engine to Secret Server (on-premise) to enable integration with Delinea Platform and leverage secret access. Only required if Secret Server (on-premise) is in use.
- Outbound access on port 443 TCP from the Secret Server (on-premise) to the Delinea Platform through Imperva ingress to support the integration.

Delinea Remote Access Service



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.

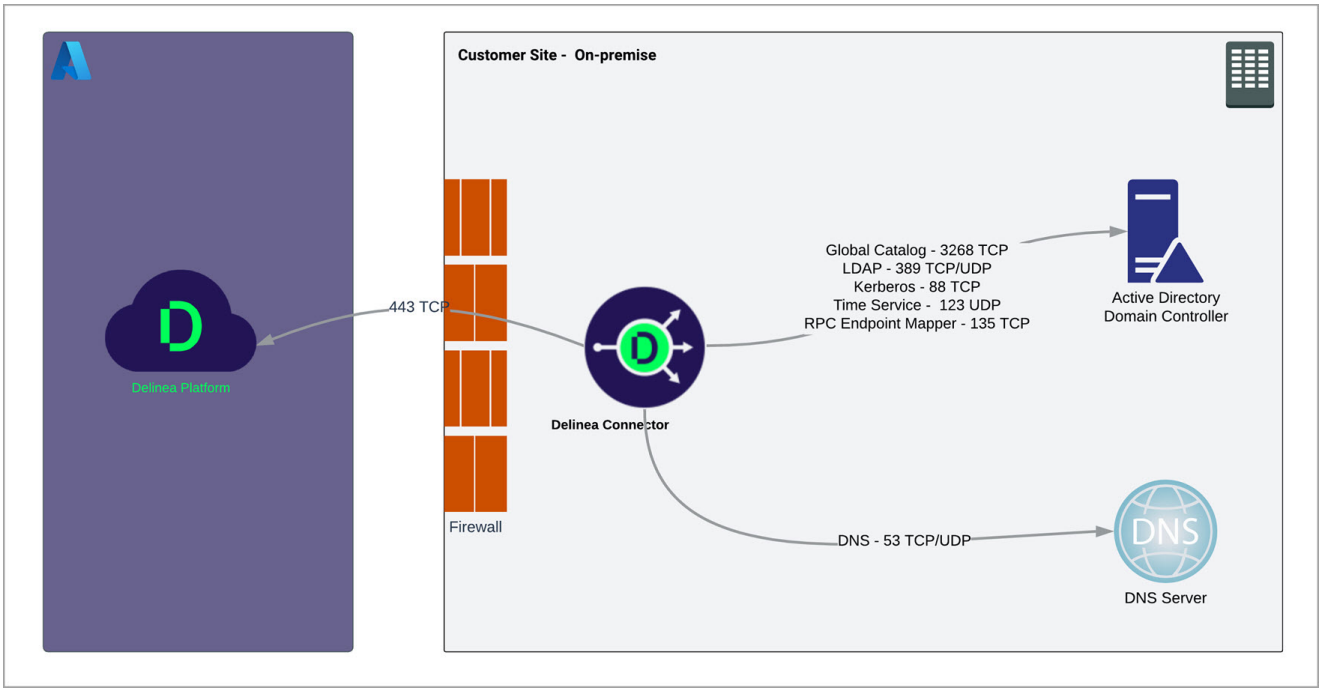
- No internet-facing ingress ports are required for the Connector
- Outbound access on port 443 TCP from the Connector to the Delinea Platform via Imperva WAF

Note: Requests from the Delinea Platform to the Delinea Connector are made via the TCP Relay hosts. Such requests for instance include querying for AD user's details. All data is encrypted.

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

- Internal access on port 3268 TCP from Delinea Connector to AD Domain Controller for Global Catalog access
- Internal access on port 123 UDP from Delinea Connector to AD Domain Controller for time synchronization
- Internal access on port 389 TCP/UDP from Delinea Connector to AD Domain Controller for handling normal authentication queries
- Internal access on port 88 TCP from Delinea Connector to AD Domain Controller used for Kerberos authentication
- Internal access on port 135 TCP from Delinea Connector to AD Domain Controller for remote procedure call (RPC) endpoint mapping
- Internal access on port 53 TCP/UDP from Delinea Connector to DNS server for name resolution (this might be the DC itself depending on your environment)

Delinea Connector



Notification Services

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

Vendor	IP Address	Purpose (examples)
AWS SES	54.240.75.72 54.240.75.73	The 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.

Supported Browsers

The Delinea Platform can accommodate most major browsers available today. We encourage users to use the latest version of a supported browser for the best experience and security on the Delinea Platform.

We support the last two stable versions of the browsers listed below:

- Google Chrome
- Mozilla Firefox
- Apple Safari
- Microsoft Edge

We do not support the following browsers:

- Microsoft Internet Explorer
- Opera

Secret Server Integration

On the Delinea Platform, secrets work the same way they do in Secret Server.

When you integrate Secret Server and the Delinea Platform, the two systems share secrets and pinned folders, as well as administrative privileges, permissions, and access settings.

Current Secret Server Customers

If you are already a Secret Server administrator and you opt-in to integration with the Delinea Platform, you will automatically gain Platform Administrator privileges while retaining all of your existing Secret Server administrator privileges. You will not gain any new Secret Server administrator privileges.

The process for existing Secret Server customers to opt-in to automated integration with the Delinea Platform can be found at the following link: Automatically Opt-in to Platform Tenant via Secret Server Cloud.

Some customers might need to manually integrate Secret Server Cloud or Secret Server On-Premises into the platform, and those instructions can be found at the links below:

- Manually Integrate Secret Server Cloud
- Manually Integrate Secret Server On Premises

New Delinea Customers

New customers who sign up for a platform trial are assigned full administrator privileges on both the Delinea Platform and the integrated Secret Server Cloud.

Opt-in to Platform Tenant via Secret Server Cloud

Automated Platform and Secret Server Cloud Integration

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, and 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 (where available) to an automatic process that provisions a new platform tenant for you and integrates it with your Secret Server Cloud instance.

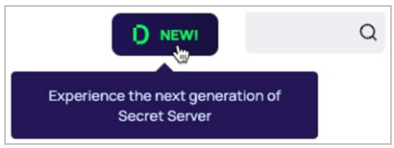
This process automatically provisions a new platform tenant and integrates it with your Secret Server Cloud instance. The integration is seamless and harmless to your current operations of your existing Secret Server Cloud instance.

Once you are in your platform tenant, all the Secret Server capabilities are provided within – including secret lifecycle management, reporting, inbox, and administration.

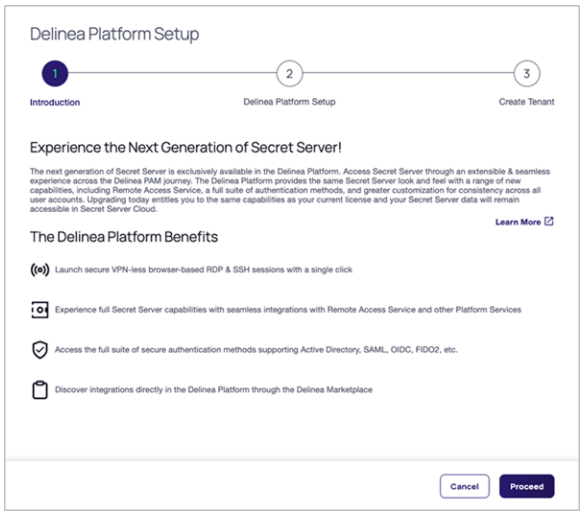
Note: Existing Secret Server administrators who become Delinea Platform administrators through the "Opt-in" mechanism retain all their existing Secret Server administrator privileges (but gain no new SS privileges) while automatically gaining Delinea Platform administrator privileges.

To get started:

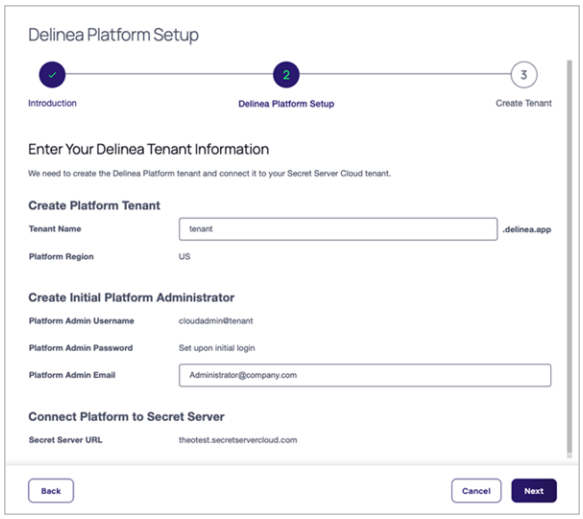
1. Log into your Secret Server Cloud instance as a tenant administrator with platform integration permissions.
2. Near the top of the portal, click the **New!** button.



A modal appears named **Delinea Platform Setup**. *Step 1* provides a brief introduction, and some platform benefit highlights.



3. Click the **Proceed** button.
4. For *Step 2*, verify that the pre-populated information is correct, and update it if necessary.

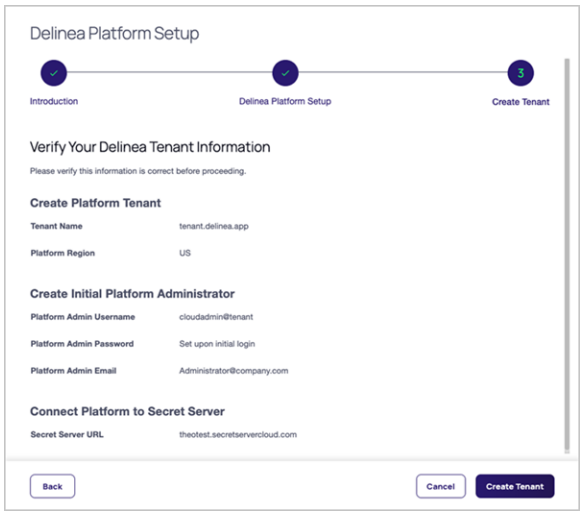


All fields are pre-populated and some cannot be changed:

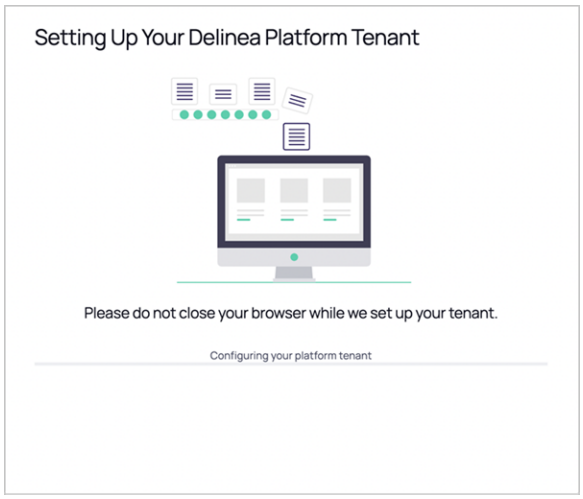
- **Tenant Name**: *Editable*. Contains the characters that precede **.secretservercloud.com** in your existing Secret Server Cloud tenant URL. Although this field is editable, we recommend accepting the default provided.
- **Platform Region**: *Editable*. Select the region that most closely matches where your Secret Server instance is located. Available Regions: US, EU, UK, Canada, Southeast Asia, and Australia.

  Note: The EU region for Secret Server Cloud is in a different location from the EU region for the Delinea Platform. For more information on the location details, please see Regional Hosting Availability
- **Platform Admin Username**: *Not editable*. The Platform Admin Username is different from your Secret Server Cloud username. It represents the platform admin user who 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, but it is editable. 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. For *Step 3*, verify that the information provided is accurate and click the **Create Tenant** button.



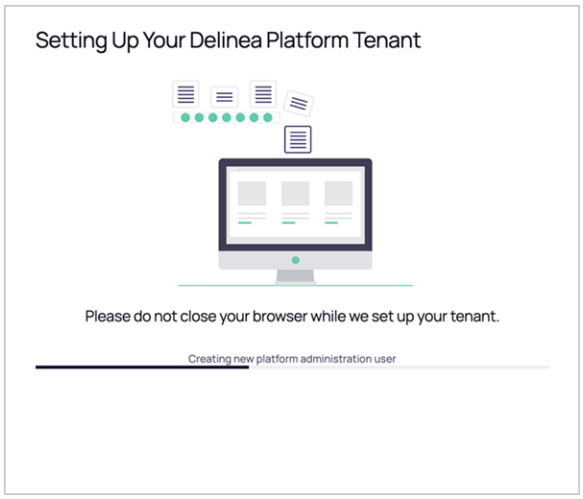
Provisioning of the platform tenant begins. A message pops up asking you not to close your browser during setup, which is typically completed in 20 seconds or less.

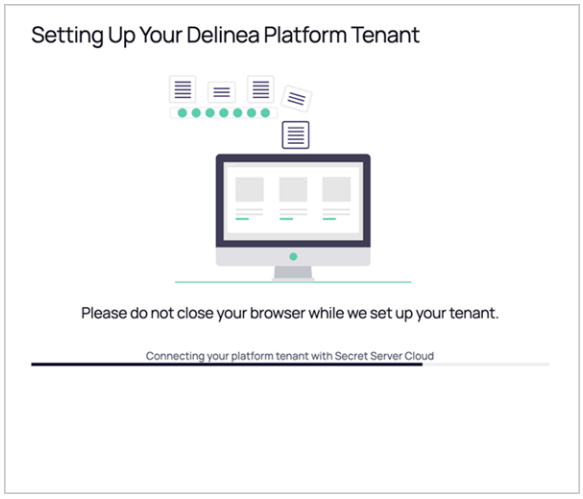


The setup process includes the following actions:

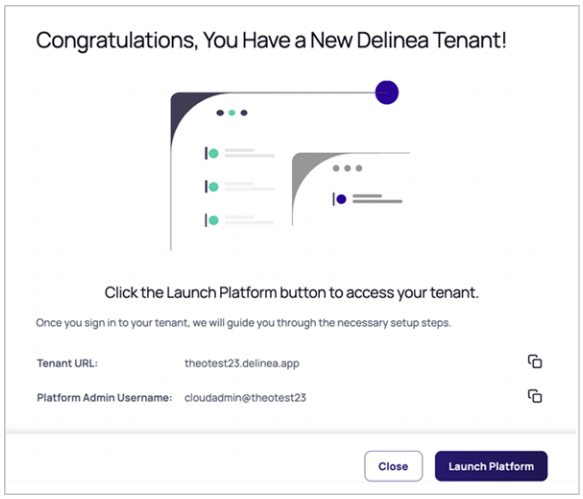
- Configuration and provisioning of your new platform tenant
- Integration of your Secret Server Cloud tenant and your new platform tenant
- Creation of the new platform administrator
- Creation and launch of an email to you with relevant information about your platform tenant.

The modal provides updates about the processes it is working on, as shown in the screenshots below:





When setup is complete, a window appears, stating **Congratulations, You Have a New Delinea Tenant!**



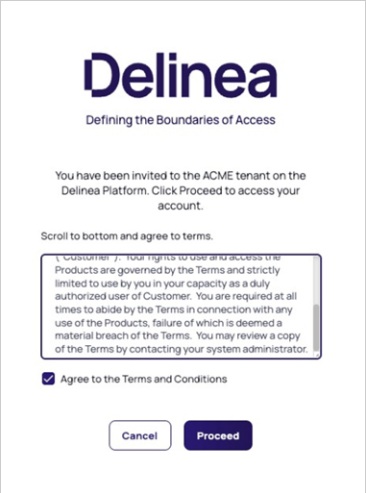
7. Click the **Launch Platform** button.

   Optionally, you can copy your platform tenant URL and bookmark it before clicking the **Launch Platform** button.

   > **Note:** If the setup process takes longer than 60 seconds, a notification appears stating, **Setup is taking longer than expected**. At this point you can wait a little longer or leave the setup process as it completes automatically, without further user input. Whether you leave or stay, the process will complete and you will receive an email notifying you that the process is finished.

Logging in and Getting Started

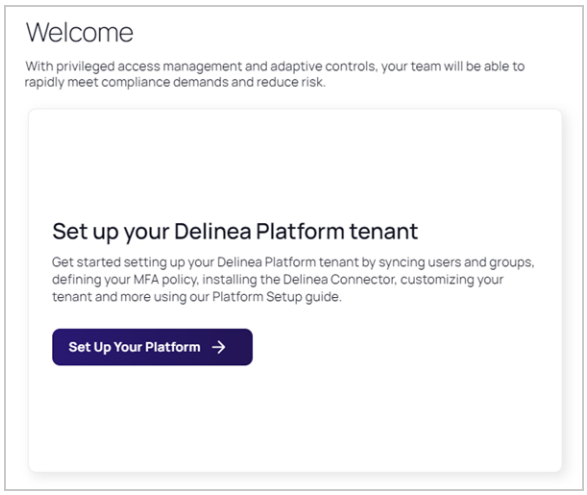
After you click the **Launch Platform** button, you will see your first login screen on your new Delinea Platform tenant.



1. Click the **Proceed** button.
2. Update your password and click the **Save** button.

You are now logged into your new Delinea Platform tenant, and your platform Welcome screen opens.

3. On the Welcome screen, click the **Set Up Your Platform** button.



The **Tasks** page opens, displaying a list of optional tasks you can take to get started using the Delinea Platform.

Use the **Learn More** links 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.

Manually Integrate Secret Server Cloud

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.

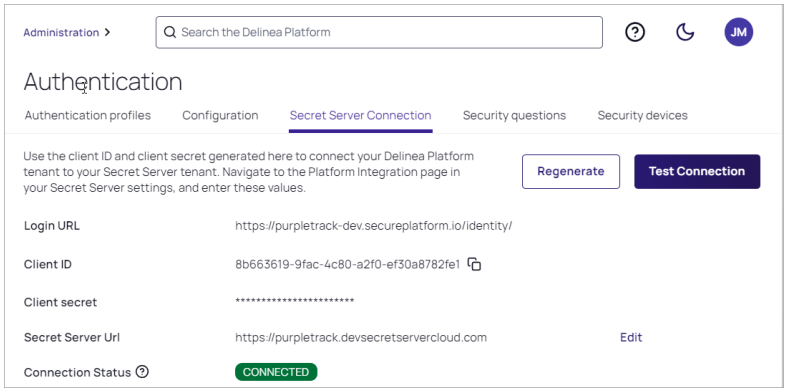
Note: Delinea platform users working with a Secret Server cloud deployment (and URL) will not see Remote Access in the top-level left navigation. The RAS engine is automatically enabled to launch remote access for secrets that are based on appropriate templates.

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 into the platform, the system checks for an existing corresponding account (by username/domain/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, then 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 into 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.



4. Copy the **Client ID** and **Client Secret** and save them somewhere 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**.

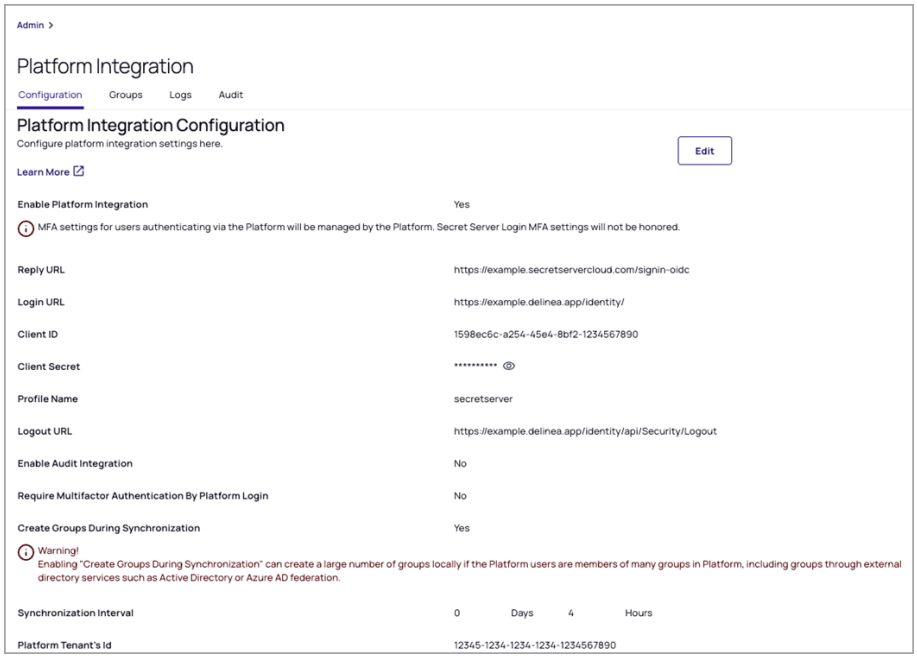
Note: If you need to regenerate the credentials (Client ID and Client Secret), please contact Delinea technical support.

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*, *Did not receive an integration response*.

Enable Platform Integration in Secret Server

1. Log into Secret Server with an administrative account.
2. Navigate to **Administration > Tools & Integrations**

3. Under **Tools & Integrations**, click **Platform Integration**.



4. Click the **Configuration** tab.
5. Input information 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`
   - **Require Multi-factor Authentication By Platform Login**: Prevents login to Secret Server from the Platform if the user has not been challenged with MFA during platform login.

     Note: This setting is strongly recommended to ensure that local users cannot bypass any MFA policies you have set for accessing Secret Server Cloud. When you set this field to **Yes**, you should immediately enable MFA for platform login. See "Identity MFA Profiles" on page 150.
   - **Create Groups During Synchronization**: Creates all the user's remote groups including directory groups
   - **Synchronization Interval**: Sets the interval for the Synchronize Platform function
   - **Platform Tenant's ID**: The platform tenant's unique identifier

> **Note:** The **Create Groups During Synchronization** setting is unrelated to the Secret Server user creation process. Secret Server Active Directory users will not show up in the platform until they try to log into the platform for the first time.

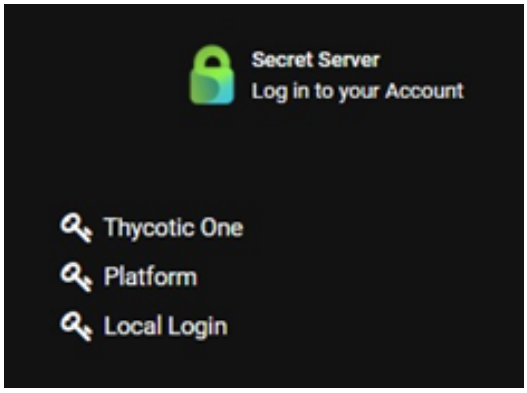
6. Check the box next to **Enabled**.
7. Once you have completed the form, click **Save**.

Verify the Integration in the Platform

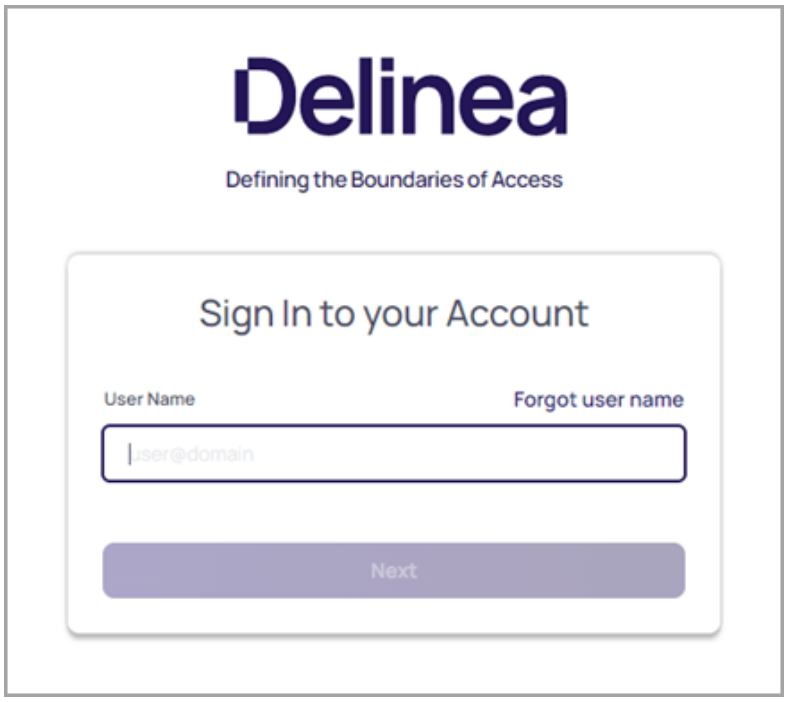
1. Log in to the Delinea Platform. If you're already logged in, log out then log back in.
2. From the left navigation menu, click **Secret Server**, then select **All secrets** from the secondary menu.
3. The **All Secrets** page displays all of your secrets from Secret Server, now shared with the platform.

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. You will be redirected to the Delinea Platform authentication portal.



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, then your integration between Secret Server Cloud and the Delinea Platform is complete.
6. Refresh the Delinea Platform page. You will now see the Secrets tab in the left navigation, and the browser launcher will appear in Secret Server.

Manually Integrate Secret Server On-Premise

The integration of Secret Server On-Premise with the platform is limited to the Remote Access use case only. Customers should expect to 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.

Accessing the Delinea Platform

Current Secret Server On-Premise customers can access the Delinea Platform and Remote Access Service 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 e-mail 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 11.4 or newer.
- An administrator account on both Secret Server On-Premise and the platform.

  Note: The platform and Secret Server On-Premise accounts must share the same login username, and the user must be logged in with this username in BOTH the platform and Secret Server On-Premise when following the steps below. This is true for any administrator accounts used for setting up the Delinea Platform and Secret Server On-Premise.

- Ensure that the network prerequisites are fulfilled to enable the integration between the Secret Server (on-premise) and the Remote Access Service feature on the Platform.

Integration Steps

1. Install a Remote Access Service engine.
2. Add a new Secret Server connection to the platform.
3. Update the platform integration settings on Secret Server.
4. Update your Secret Server connection with the RAS site.
5. Verify the overall integration.

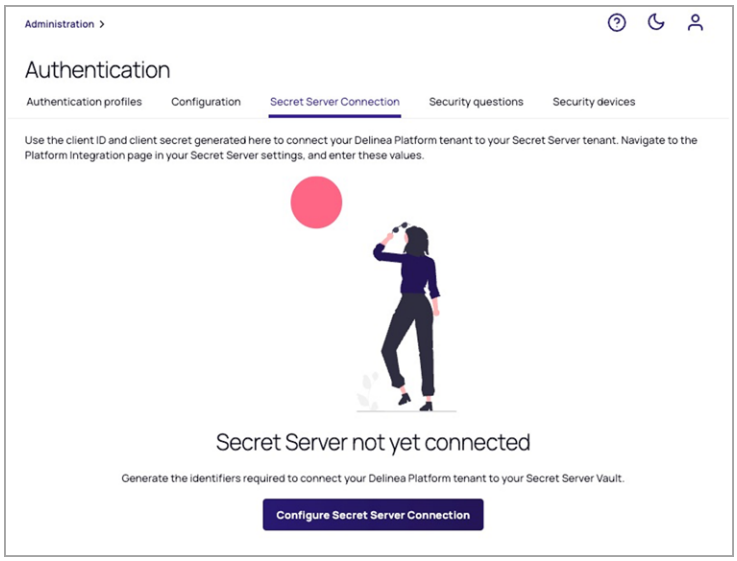
Install a Remote Access Service Engine

Deploy a Remote Access Service (RAS) Engine and ensure that the RAS Engine has access to your Secret Server On-Premise instance.

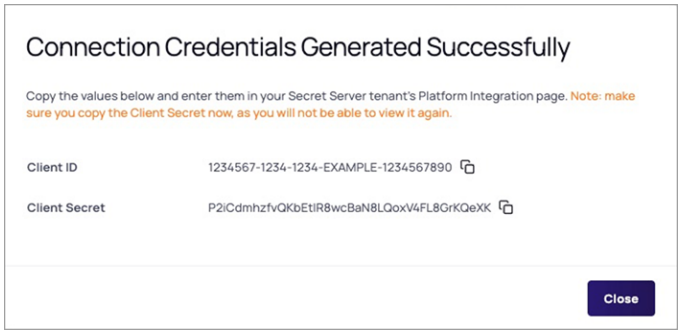
1. Log in to the platform.
2. Click **Settings** from the left navigation, then select **Remote Access**.
3. Follow the steps in Remote Access Service on installing a RAS Engine.

Add a New Secret Server Connection

1. Log in to the platform.
2. Click **Settings** from the left navigation, then select **Authentication profiles**.
3. Select the **Secret Server Connection** tab.
4. Click **Configure Secret Server Connection** to generate the required connection credentials.



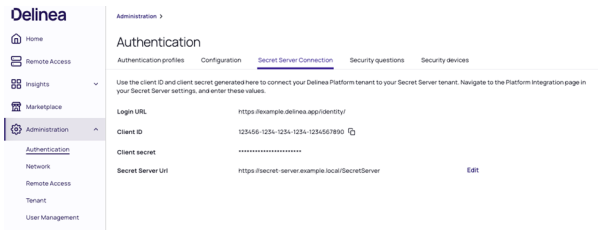
The platform will generate a Client ID and Client Secret.



5. Make note of the Client ID and Client Secret values, because you will need them later.

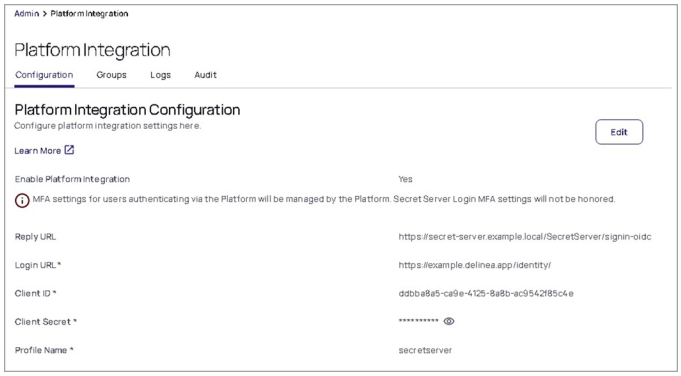
   Note: If you need to regenerate the credentials (Client ID and Client Secret), please contact Delinea technical support.

6. Update the Secret Server URL field, in the format, `https://<hostname or IP address>/SecretServer`. For example, `https://secret-server.example.local/SecretServer`.



Update the Platform Integration Settings On Secret Server

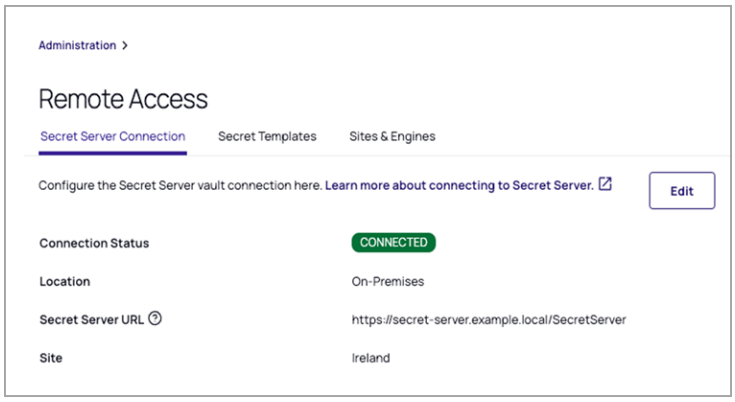
1. Log in to your Secret Server On-Premise instance.
2. Navigate to **Administration** > **Platform Integration**.
3. Click **Edit**.
4. Update the following settings:
   a. **Login URL**: the platform login URL that you copied from the earlier step
   b. **Client ID**: the identifier assigned part of the OIDC connection
   c. **Client Secret**: a secret used by Secret Server to authenticate with the platform



Update Your Secret Server Connection with the RAS Site

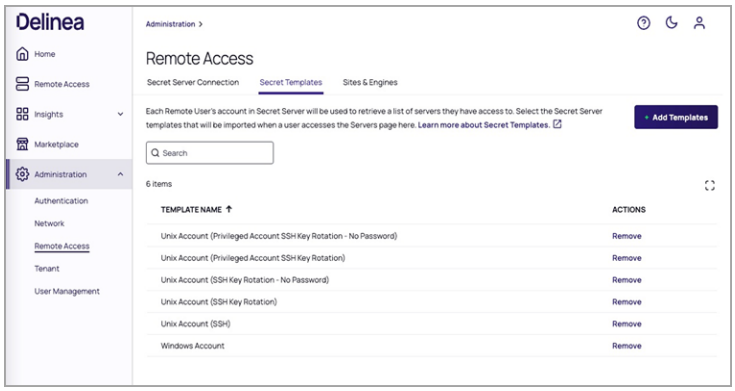
After the RAS engine is successfully installed, perform these steps:

1. Navigate to **Administration** > **Remote Access** > **Secret Server Connection**.
2. Click **Edit**.
3. Update the **Site** field with the RAS site that contains the engine you just created.

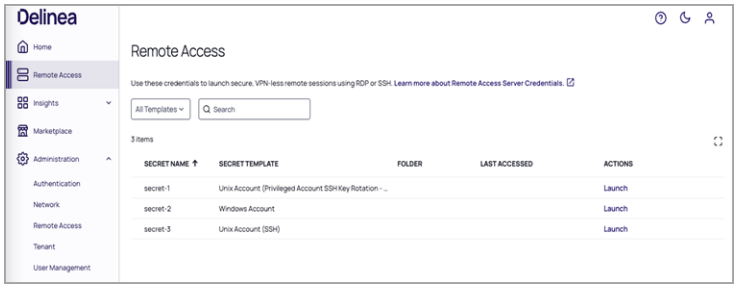


Verify the Overall Integration

1. Log in to the Delinea Platform.
2. Navigate to **Administration** > **Remote Access** > **Secret Templates**. A default set of Secret Server templates should appear here. You can add others as desired by clicking **Add Templates**.



3. Click **Remote Access** from the left navigation menu. Typically, secrets created by or shared with the logged-in user should appear here.



You can now launch Remote Access sessions from the secrets that support RAS by clicking the **Launch** link under the **Actions** column.

Delinea Connector

The Delinea Directory Connector enables secure communication between the Delinea Platform and AD directories.

Determining whether you need the Delinea Connector

The Delinea Connector serves as 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:

- If you intend to use Active Directory (AD) as the identity repository for authenticating users on the Delinea Platform.

- If you consider Integrated Windows Authentication (IWA) to be an adequate method for Active Directory user accounts to access the platform.
- If you wish to prompt users for RADIUS Multi-Factor Authentication (MFA), allowing your RADIUS server to verify users on the Delinea Platform. In this scenario, the Delinea Connector functions as a RADIUS client.
- If you consider using Privilege Control for Servers.

For enhanced reliability and efficiency, it is recommended to deploy multiple connectors to enable fail-over capabilities and load distribution.

Installing the Delinea Connector

Requirements

Platform Permissions: To generate a connector registration code or manage the connector settings, you must belong to the Administrator group on the platform.

Connector Permissions: To install and register the connector, you must be a local administrator on the machine where you are installing connector, so that you can copy files to Program Files, set up Windows service, and write settings to registry.

The connector Server: The server or virtual machine where the Delinea Connector is installed must be:

- Always running and accessible on the internal network
- Running Windows Server 2019 or newer
- Running 64-bit with 8 GB of memory or more, of which 4 GB or more should be available for connector cache functions.
- Running Microsoft .NET version 4.8 or newer; if it isn't already installed, the installer installs it for you, but in this situation, you must manually restart your machine (restart is not forced) to complete the connector installation.
- If the connector is integrating with an on-premises Active Directory, the machine where it is installed must be joined to Active Directory (AD) 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" on page 17. 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 best practice avoid installing the connector on a domain controller.

Permissions Required for Alternate Accounts and Organizational Units

You can run the Delinea Connector service as an Active Directory service account instead of as a Local System account. The account you select must have all required permissions. For example, if you run the connector service as a specific Active Directory service account, the account must be a member of the local Administrators group, and it must have at least read permission to the container with platform user accounts and Active Directory Groups used

as members of platform groups. The account also requires 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 may not. This most often occurs in multi-forest or multi-domain setups and can occur even when two-way trust is already defined. You can tell when this occurs because the connector log would show the error message, Unable to locate forest or user object. In this case, you need to give the Local System account read access permission to the containers or organizational units.

Set 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 click the **Allow** box 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.

Downloading the connector and getting a registration code

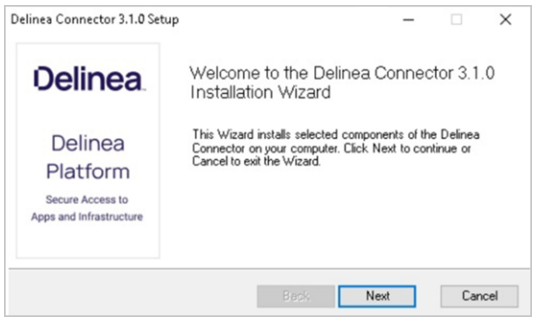
To download the connector, follow these steps:

1. Log into the Delinea Platform.
2. Click **Settings** from the left navigation, then click 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.

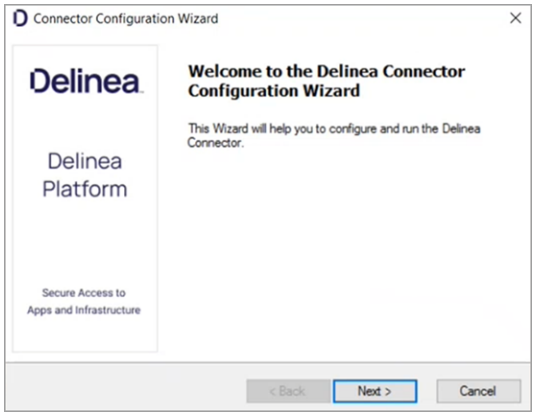
> **Note:** The auto-generated registration code is created with default values only. It does not have an expiry time or limits on how many times the registration code should be used.

Installing and configuring the connector

1. On the *Delinea Connector machine*, run the connector Installer file you downloaded in the last section. The connector Installation Wizard launches.

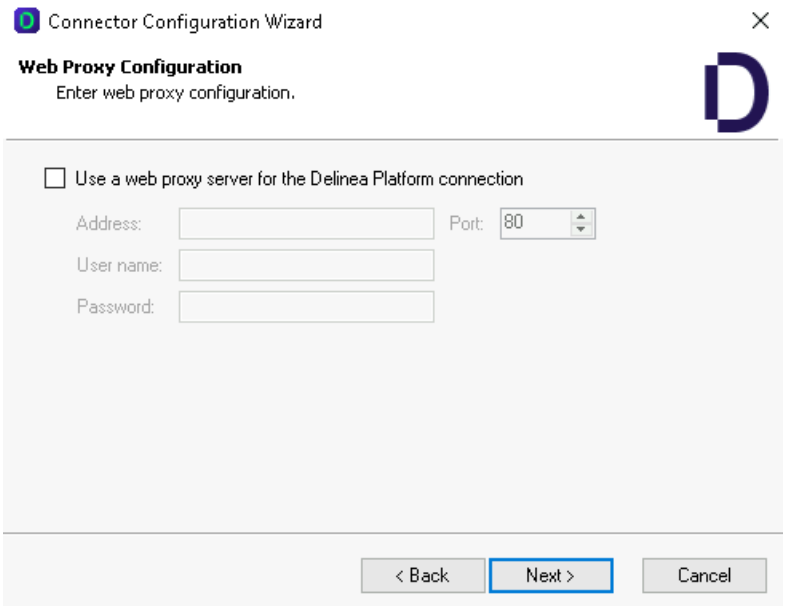


2. Click **Next**.
3. Click the Connector tab.
4. Click **Register**. The connector Configuration Wizard launches.

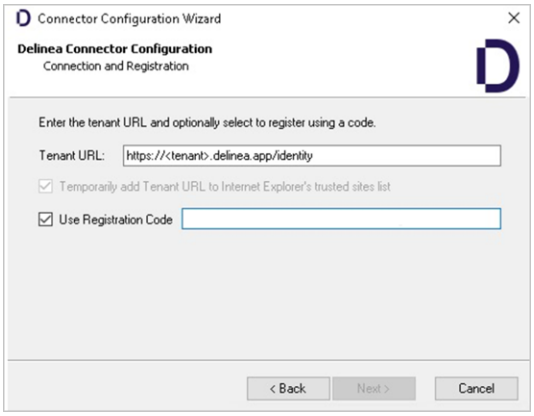


> During the configuration process, we recommend keeping default settings except where these instructions indicate otherwise. You can choose to configure the connector to change TLS to 1.2 for every .net app on the machine globally.

5. Click **Next**.
6. Select the box next to **Enable strong encryption protocols system-wide**.
7. If you are using a web proxy server to connect to the platform, select the box next to **Use a web proxy server for the Delinea Platform connection** and specify the **IP Address**, **Port**, **User name**, and **Password** to use.



8. Click **Next**.



9. In the **Tenant URL** field, paste the tenant URL you copied and saved earlier.
10. Select the box next to, **Temporarily add Tenant URL to [browser's] trusted sites list**.
11. Select the box next to **Use Registration Code**.
12. Paste the registration code you copied and saved earlier into the **Use Registration Code** field.
13. **This step is optiona**l: 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, then run this command:

    ```
    dsacls "CN=Deleted Objects,DC=\<EXAMPLE\>,DC=\<COM\>" /takeownership
    ```

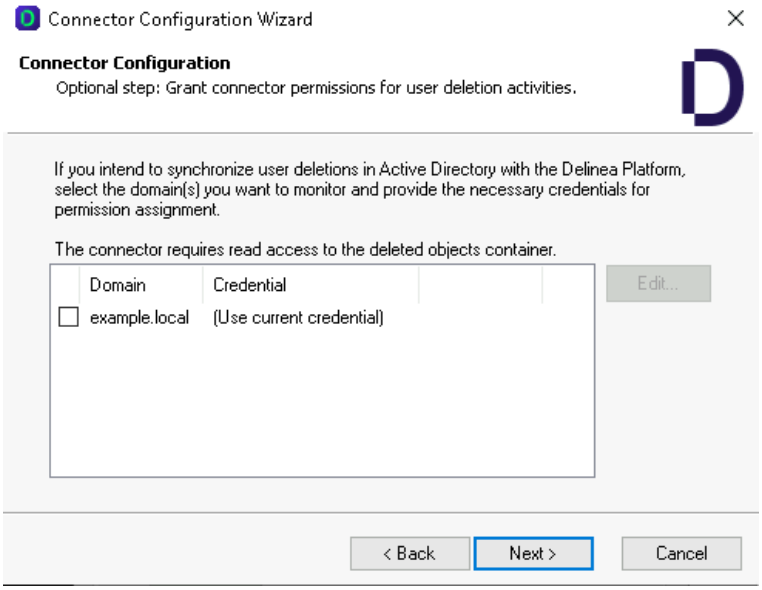
    Potential Results:

    - The command completed successfully
    - The command failed to complete successfully
  - The following command grants the Delinea Connector permission to read the deleted objects container in Active Directory:

    ```
    dsacls "CN=Deleted Objects,DC=\<EXAMPLE\>,DC=\<COM\>"
    /user:administrator@\<EXAMPLE.COM\> /passwd:\* /g
    \<EXAMPLE\>\\\<MACHINENAME\>\$:LCRP /I:T
    ```

    If this command fails, it means 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 re-run the steps again.
- Apply read permissions to the service account for the deleted objects container in the corresponding domain.

> Failure to perform any of the actions mentioned above will result in users deleted in Active Directory being still listed on the Users page in the platform until you manually remove them. However, these users will not have access to any platform functionalities.

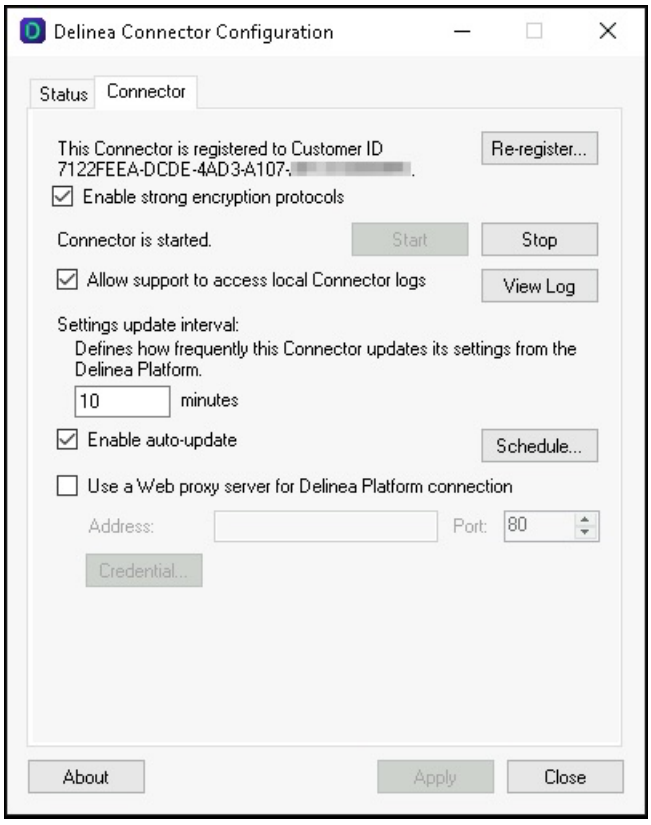


14. Click **Next**. The wizard performs checks to validate the network environment.
    Wait for the checks to complete.
15. Click **Next**. The next screen displays a bar indicating the progress of the configuration. Wait for the bar to be full.
16. Click **Next**. You should see a notice saying, connector setup is complete.
17. Click **Finish**.

Enabling auto-update for the 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.

1. Log in to the Delinea Connector server.

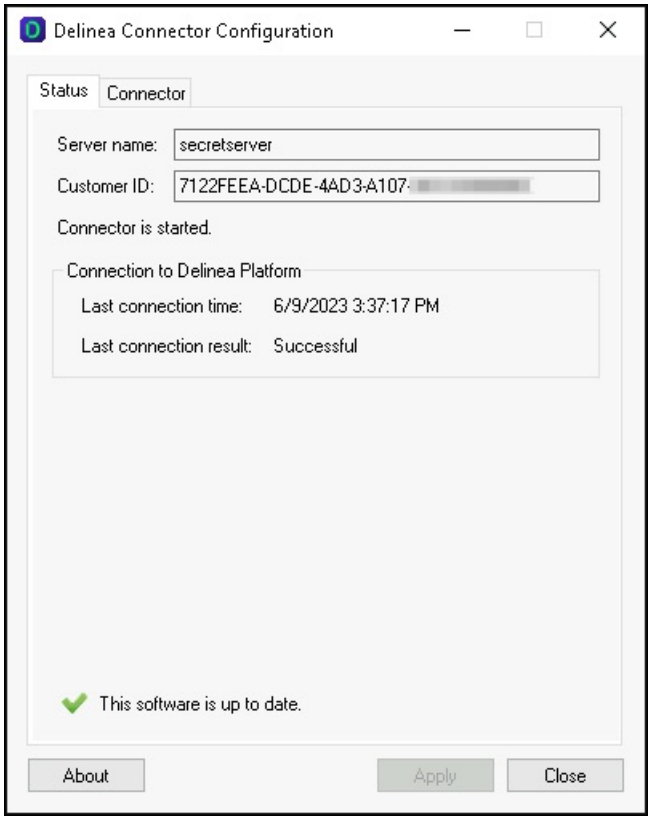


2. Click the Windows Start menu and open the Delinea Connector Configuration program.
3. Use the **Enable auto-update** check box to enable automatic updates.
4. Use the **Schedule** button associated with the *Enable auto-update* option to configure the auto-update time window.
5. Click **Apply**.

Updating the connector

1. Click the Windows Start menu and open the Delinea Connector Configuration program.
2. In the lower left of the **Status** tab, right-click the update icon and select **Update**. The connector updates and

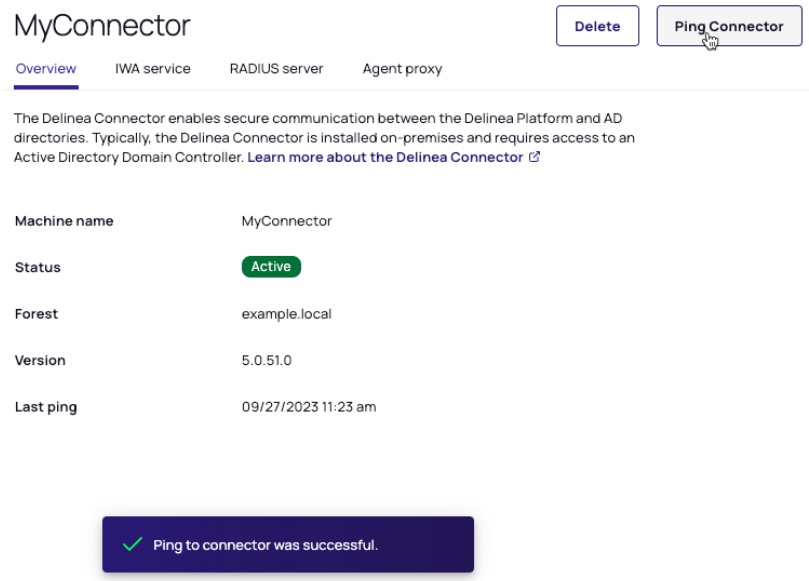
displays a message, indicating that the software is up to date.



Checking connector status

To verify the status of the connector, click the **Ping connector** button.

If all components are functioning correctly, a success banner will announce, *Ping to connector was successful*. If any communication issues are detected between the platform and the connector, an error message will be displayed. The timestamp for the last ping will be updated to reflect the most recent successful ping check.



Connector Best Practices

Supporting user authentication for multiple domains

You install the connector on a machine that is joined to Active Directory (AD) to authenticate Delinea Platform users who have an account in that domain. If you want the Delinea Platform to authenticate users in other domains, there are two connector installation models. The choice of model depends on whether the accounts are in trusted domains within a single forest or in multiple forests without trust.

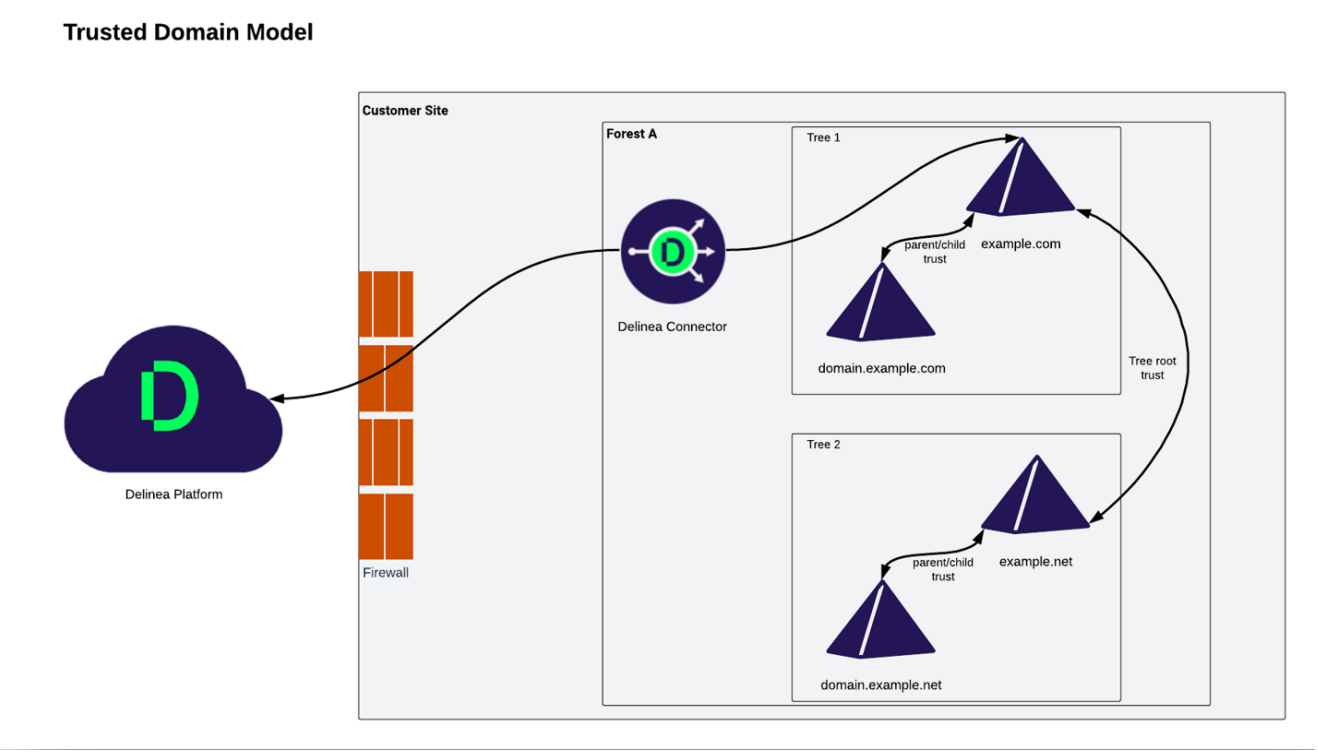
If all your Delinea Platform users have their accounts in a single domain controller, you can skip this topic.

Configuring authentication for trusted domains

You use this model 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 model, you have just 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 connectors" on page 46.

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.



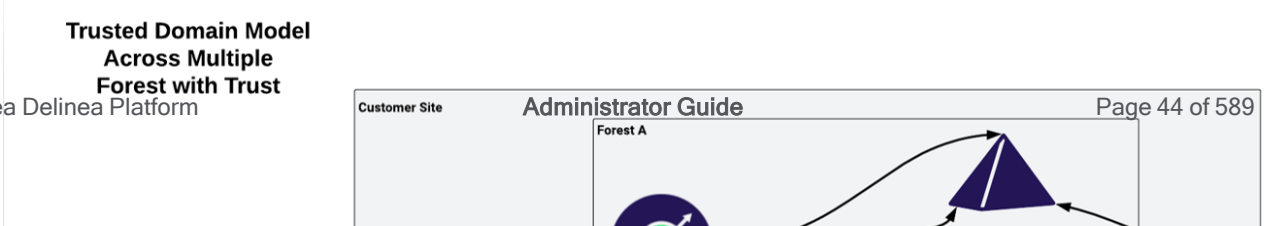
By default, two-way transitive trusts are automatically created when a new domain is added to a domain tree or forest root domain using the Active Directory Installation Wizard. The two default trust types are parent-child trusts and tree-root trusts. When configuring the trust relationship, ensure to select Forest Trust. This action 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 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 "Delinea Connector" on page 34.

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 platform portal, it only searches the Active Directory Users container in the domain controllers visible to the connector.

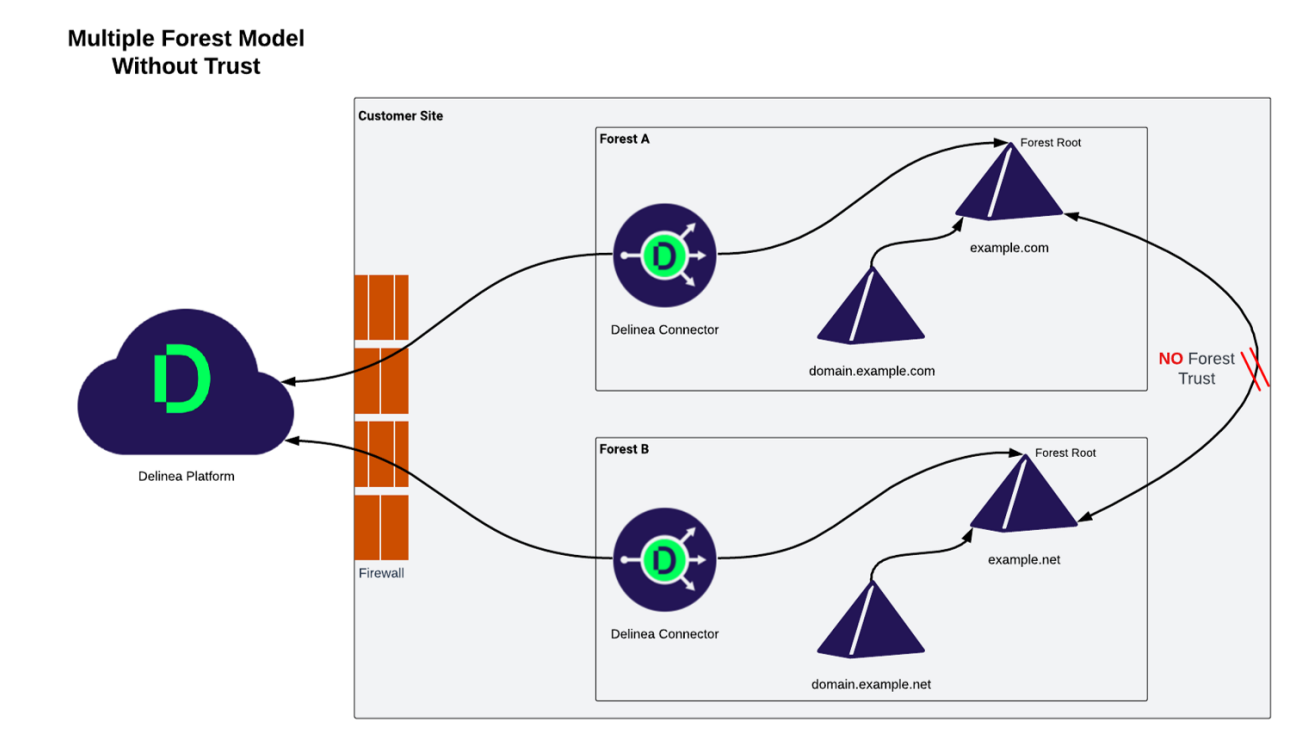
Important: By default, the connector does not perform cross forest user look-up from a local forest. To enable this functionality, please reach out to Delinea Support team. Once enabled, avoid installing connectors in each of the forests where trust exists. For example, if you decide to run connectors 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, as they're seen as separate entities within each forest, making the resolution of such issues challenging.



Configuring authentication for multiple forests without trust

When you use this model, it applies to scenarios where users' Active Directory accounts are in multiple forests without trust such as in restricted access forest model or when you have distinct forests due to organization or administrative boundaries (e.g. mergers, separate business units, etc.)

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.



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, refer to the section on "Installing additional 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 platform portal 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, refer to "Delinea Connector" on page 34.

Connector redundancy

To ensure continuous up time 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. This means that 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 connectors

You use the same procedure to download the installation wizard to the host server and then run the wizard to install and register additional connectors. After you install and register the connector, it is added to the Delinea Connector settings page.

See "Downloading the connector and getting a registration code" on page 36 for more information.

Additional information

- AD changes are pushed from the connector to 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 either universal or security AD groups.
- To automate the installation process of the Delinea Connector, visit the Delinea GitHub repository for more information. 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.

Troubleshooting the Connector

Issue: While installing the Connector, I get this error message: *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 "Delinea Connector" on page 17 are allowed.

Issue: While installing the Connector, I get this error message: *Failed to obtain certificate or certificate verification failed.*

Resolution:

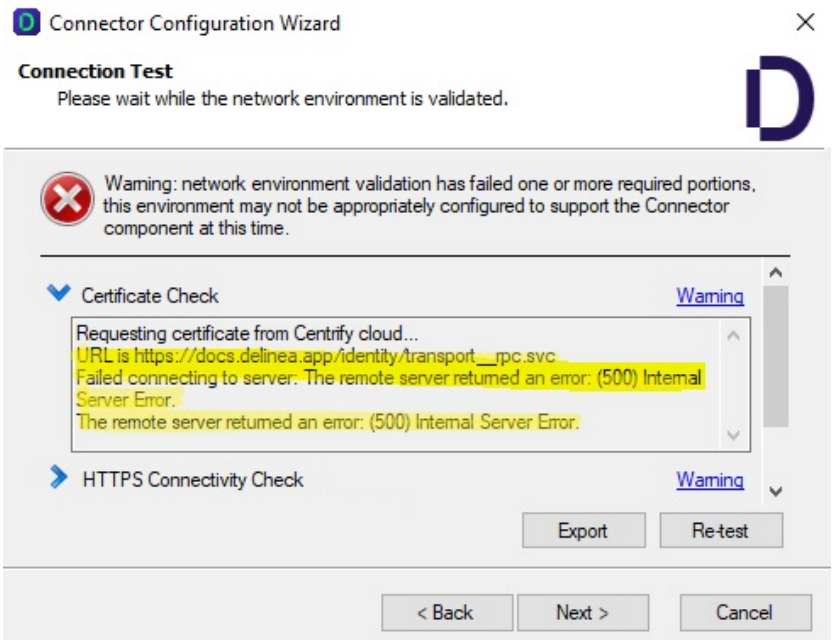
1. Make sure your Windows updates are up to date.
2. Verify the accessibility of Certificate Revocation Lists (CRLs) by confirming access to the following:

- http://cps.letsencrypt.org
- http://x1.c.lencr.org/

Issue: While registering the Connector, I get this error message: *Encountered unhandled exception in registering the proxy: System.ServiceModel.EndpointNotFoundException: There was no endpoint listening at http://<tenant url>/transport_rpc.svc*

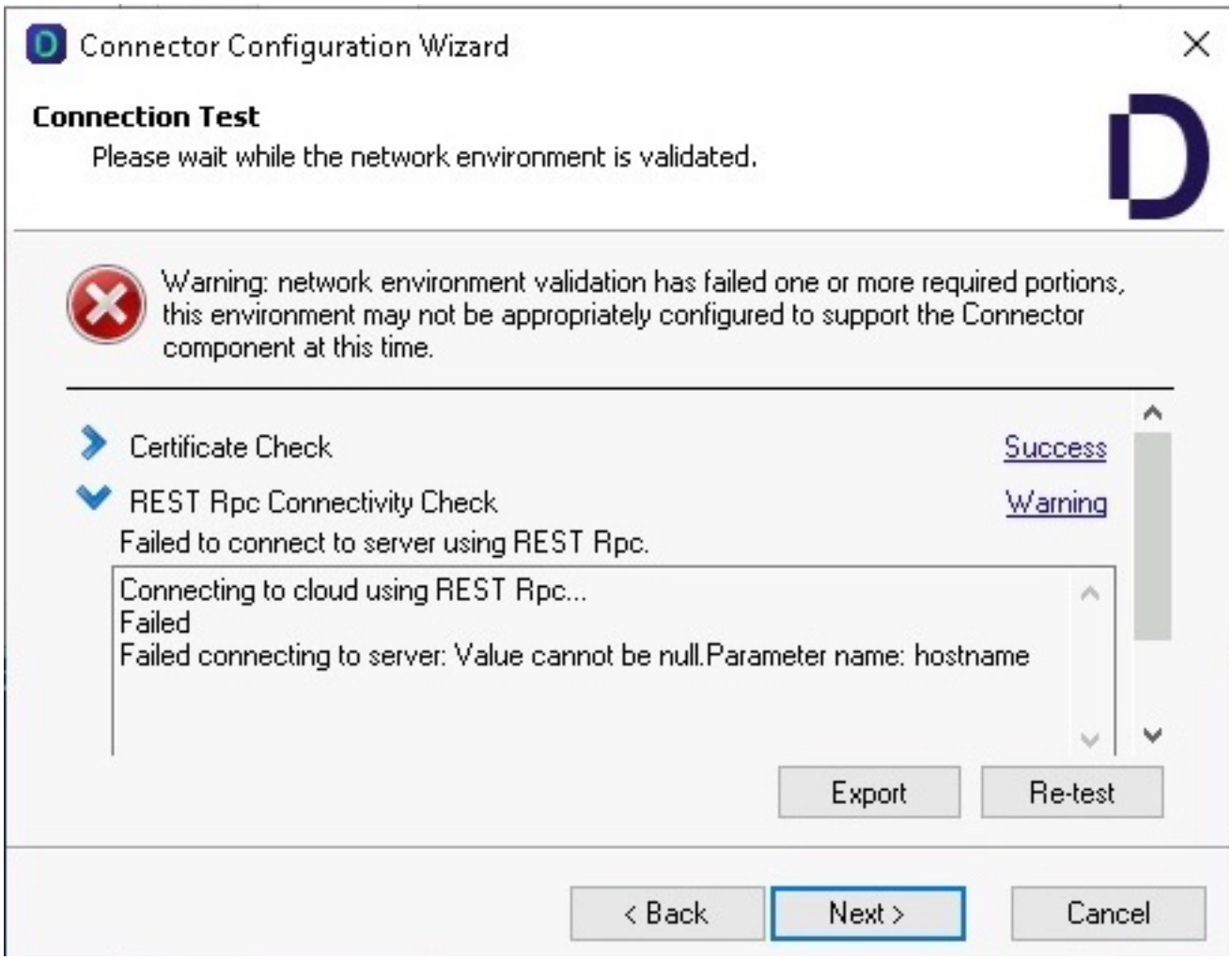
Resolution:
Ensure that you are running the latest version of the Connector and try again.

Issue: While registering the Connector during certificate checks validation, I get this error: *(500) Internal Server Error*



Resolution:
Ensure that you are running the latest version of the Connector and try again.

Issue: While registering the Connector, I get this error message: *Failed to connect to server using REST RPC*



Resolution:
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.

Issue: After starting the Connector Configuration application, nothing happens for several minutes and the application is not accessible.

Resolution:
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.

Issue: The Connector fails to connect to the platform.

Resolution:
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 "Delinea Connector" on page 17. 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.

Issue: Auto-update isn't working for my Connector

Resolution:
AutoUpdate support was added after 4.1.x versions. Manually upgrade to the latest version of the Connector to take advantage of auto-update.

Issue: The Connector is correctly installed and active, but AD users can't log in and they get this error message: *Authentication (login or challenge) has failed. Please try again or contact your system administrator.*

Resolution:

- Verify that the user is entering accurate Active Directory credentials to log in to the platform.
- Examine the 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.

Issue: I don't know where to access the Connector logs.

Resolution: Connector logs (e.g. log.txt) can be reviewed under C:\Program Files\Delinea\Delinea Connector

Issue: I don't know the default log rotation setting for the Connector logs

Resolution: The default maximum log file size is 2 MB, and the default maximum number of log backup entries is 450.

Issue: I want to use both Federation and Active Directory (AD) with the platform, but I don't know the best practices for doing this.

Resolution:

1. First set up the Connector first, 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.

Issue: I can't query Active Directory users or groups from the platform, despite having an active connector.

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."

Resolution:

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.

Federation

A federation service enables users to log onto the Delinea Platform using credentials from a trusted third-party federated identity provider (IdP). 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 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)

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

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, you can still configure it using your official IdP provider documentation and the information provided here.

- "Integrating Auth0" on page 60
- "Integrating Microsoft Entra ID" on page 70
- "Integrating Entrust" on page 94
- "Integrating Okta" on page 107
- "Integrating OneLogin" on page 121
- "Integrating Ping Identity" on page 132

SP-Initiated vs IdP-Initiated SSO

SSO simplifies user access across multiple applications with a unified login. There are two approaches:

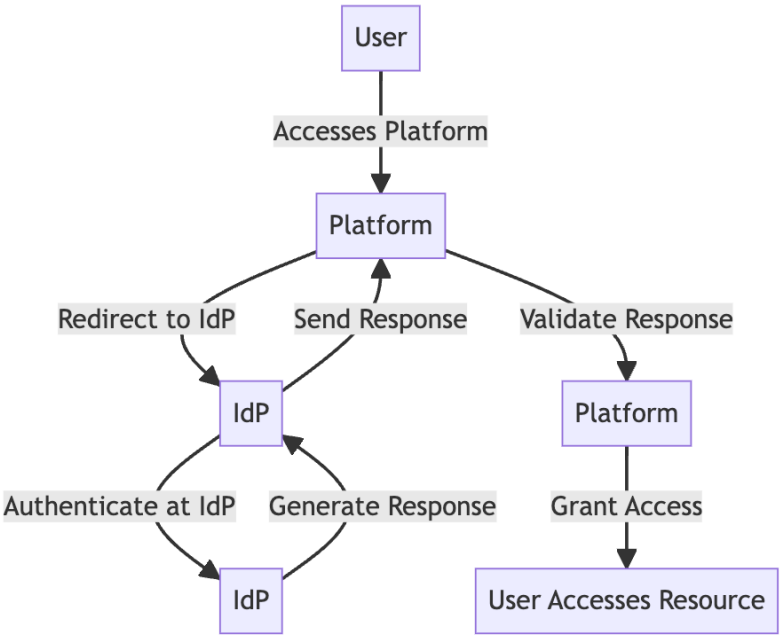
- SP-initiated SSO
- IdP-initiated SSO

Each approach serves specific organizational needs and IAM architectures. The Delinea Platform supports both.

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 overarching sequence of actions in SP-initiated SSO at a high level. It is important to note that the specific steps of these flows may vary depending on the chosen SSO protocol, such as SAML or OpenID Connect.

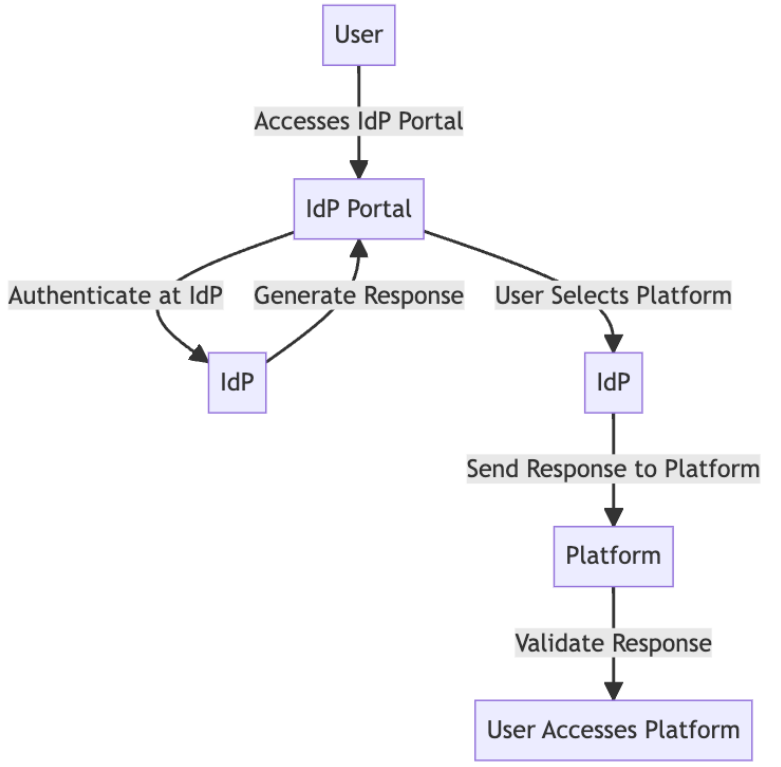


1. The user starts by accessing the Delinea Platform (SP in this case).
2. The platform redirects the user to the Identity Provider (IdP) for authentication.
3. The user authenticates at the IdP.
4. The IdP creates an authentication response.
5. This response is then transmitted from the IdP to the platform.
6. The platform validates the response and grants the user access to the Delinea Platform.

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 overarching sequence of actions in IdP-initiated SSO at a high level. It is important to note that 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.

Federation Management

Add a Federation Service Provider

1. From the left navigation, click **Settings**, then select **Federation providers**.
2. Select Federation providers from the secondary menu.
3. On the Federation Providers page, click the **Add Provider** button.
4. Select SAML or OIDC. The Add Provider page opens, displaying all controls necessary for adding a provider.

Consult the detailed documentation for these specific IdPs:

- "Integrating Auth0" on page 60
- "Integrating Microsoft Entra ID" on page 70
- "Integrating Entrust" on page 94
- "Integrating Okta" on page 107
- "Integrating OneLogin" on page 121
- "Integrating Ping Identity" on page 132

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 deletion. Please 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 (SAML only)

Customize Certificate Issuer Sent to IDP: This setting overrides the default Certificate Issuer (also referred to as the Entity ID) information sent to the Identity Provider (IdP). Please note that this setting should be used cautiously and only when necessary to maintain compatibility with your IDP configuration.

ForceAuthN: Select the box to force authentication, or deselect the box to disable forced authentication. When enabled, the Force Authentication (ForceAuthN) setting asks the identity provider (IdP) to require the user to *re-authenticate*, even if they have an existing session or have 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 by 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.

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 where 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 platform, the user's overall session with the IdP is not impacted or invalidated.

Prompt for Re-authentication (OIDC only)

1. On the provider's page click **Edit**.
2. Under **Settings**, set the **Prompt** setting to the desired option.

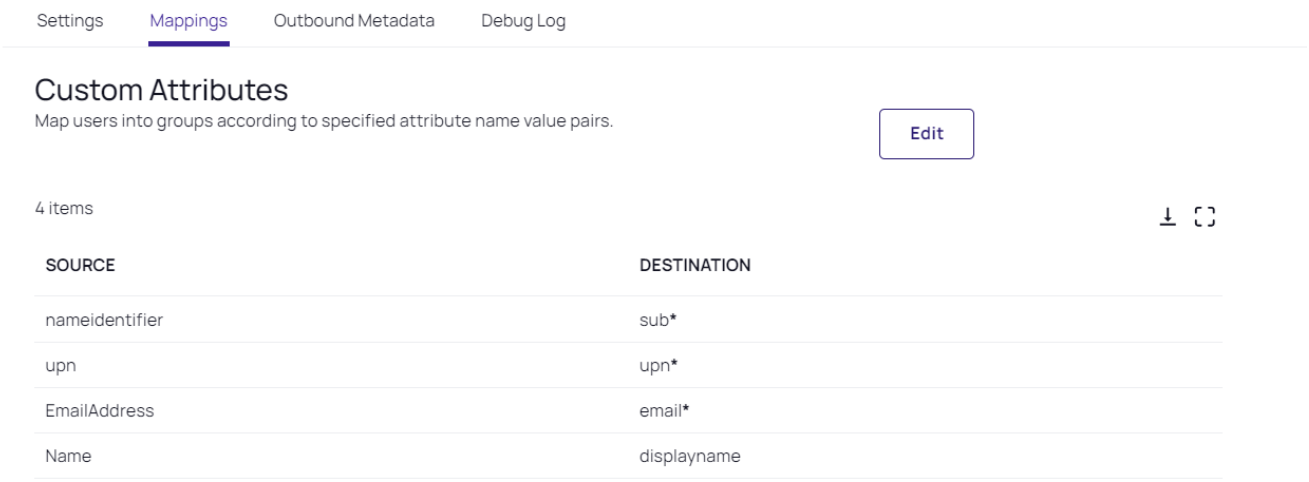
Support for these options depends on the OIDC implementation used by the IdP.

Option	Description
Not specified	Default option. If the user has a valid authentication session with their IdP, they will not be re-prompted to authenticate. If the user is not authenticated or has no active session, they will be redirected to the IdP to initiate the authentication process.
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 re-authenticate with their IdP, 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 out of the box, and new, custom attributes can be added.

The screen shot below provides an example set of custom attributes for SAML with Auth0.



The attributes below are mandatory for proper setup of federation on the Delinea Platform:

- "sub": Name Identifier. Corresponds to unique identifier of the user.
- "upn": User Principal Name. Attribute that specifies a user account logon name.
- "email": Email Address. Corresponds to the email address of the user.

Optionally, these additional user attributes can be mapped on the platform:

- **DisplayName**: Display name (e.g., John Smith). While the *displayname* attribute is optional, it is advisable to include it for optimal results.
- **MobileNumber**: Corresponds to the user's mobile phone number.
- **OfficeNumber**: Corresponds to the user's office phone number.
- **HomeNumber:** Corresponds to the user's home phone number.
- **Description**: Allows for additional descriptive text.

Custom attributes for IdP federation can vary depending on the specific IdP, so consult the documentation and support resources of your chosen IdP.

Group Mappings

Group mapping is the method of associating user groups from an IdP such as Auth0 to corresponding local groups on the Delinea Platform (SP). This ensures that the user is granted the appropriate level of access based on their group memberships in the IdP's system.

Administrators can define mappings that dictate how the groups received from the IdP should be translated into specific groups on the platform.

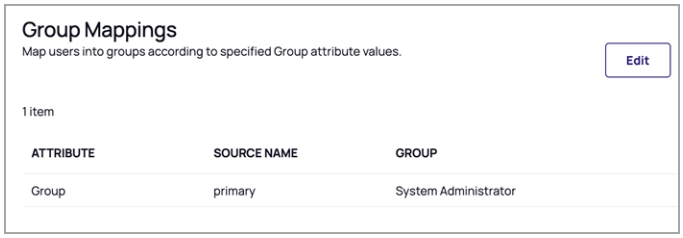
On the Delinea Platform, federated groups are not *added* to named platform identity groups. Instead, they are *mapped* to platform groups through the IdP group's *Object ID*.

When a user logs in with an IdP's federated email domain, the platform will log them in as a federated user. The user is first authenticated when the IdP sends the platform an attribute/claim named `groups` for that user, which

includes an Object ID for each IdP group that user belongs to. The Object ID maps to platform groups, and the user is added as a member of those mapped groups.

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 as described below. For more information on groups, roles, and permissions, see User Roles and Permissions.

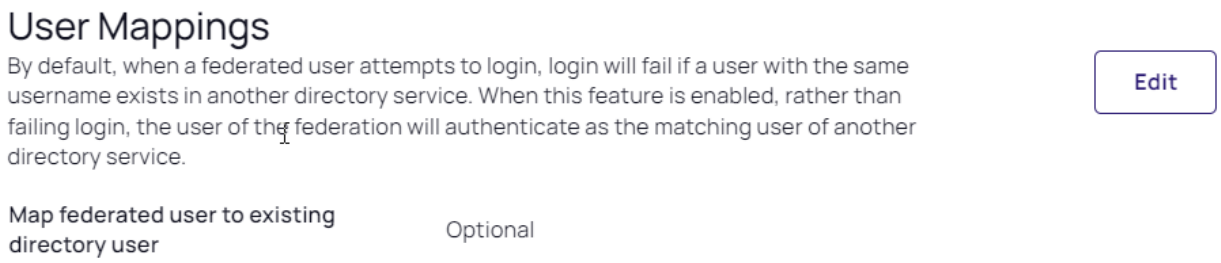
The following screen shot shows an example of a group attribute with the group `primary` received from the IdP, which is mapped to the System Administrator local group on the Delinea Platform.



User Mappings

User mapping is the process of associating user identities between an Identity Provider (IdP) such as Auth0 and any existing user on the Delinea Platform (SP) irrespective of directory source.

Optional: In the default platform configuration, when a federation user attempts to authenticate, the platform maps the user to an existing account in either the local directory or Active Directory, 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.

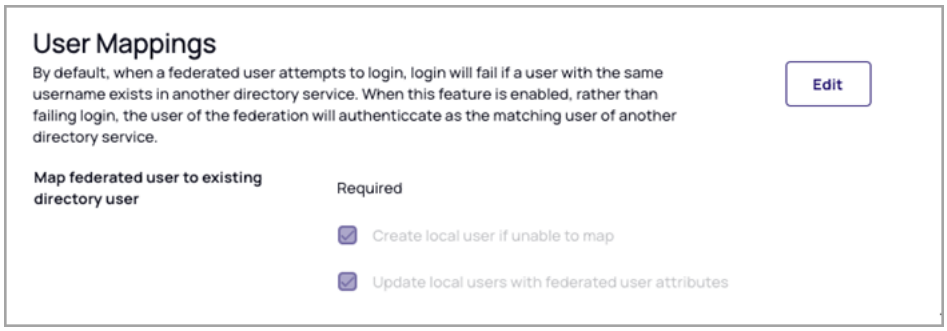


Disabled: When user mapping is disabled, a federated user's login attempt will fail if a user with the same username exists in another directory service.

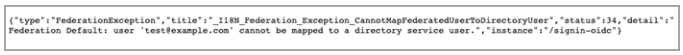
Below is an example of an error that occurs when attempting to log in to the platform causes a collision between a federated user and one or more other users with the same UPN that may exist on the platform.

{"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"}

Required: Selecting this option means the user of a federation will authenticate as the matching user of another directory service (local or Active Directory). If no match is found, login is denied.



If the user mappings are set to "Required" and no option is selected, and there is no existing user on the platform that matches the federated user, the federated user's login attempt to the platform will fail, accompanied by an error message similar to the following:



If the option "Create cloud user if unable to map" is selected 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 logins.

By opting to enable "Update cloud users with federated user attributes" you can guarantee that the mapped Delinea Directory user attributes consistently receive updates based on the federated assertions.

Debugging Federation Setups

The Delinea Platform offers a self-service debugging tool for troubleshooting federation setups with IdPs. The user-friendly interface empowers administrators 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 will change 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 will appear in a row displaying session details described in the table below. You can expand the entry to review additional details.

Column	Description
Timestamp	The date and time for the federated user's login event.

Column	Description
Email	Email address associated with the federated user.
UPN	User Principal Name; represents the federated user's identify.
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.

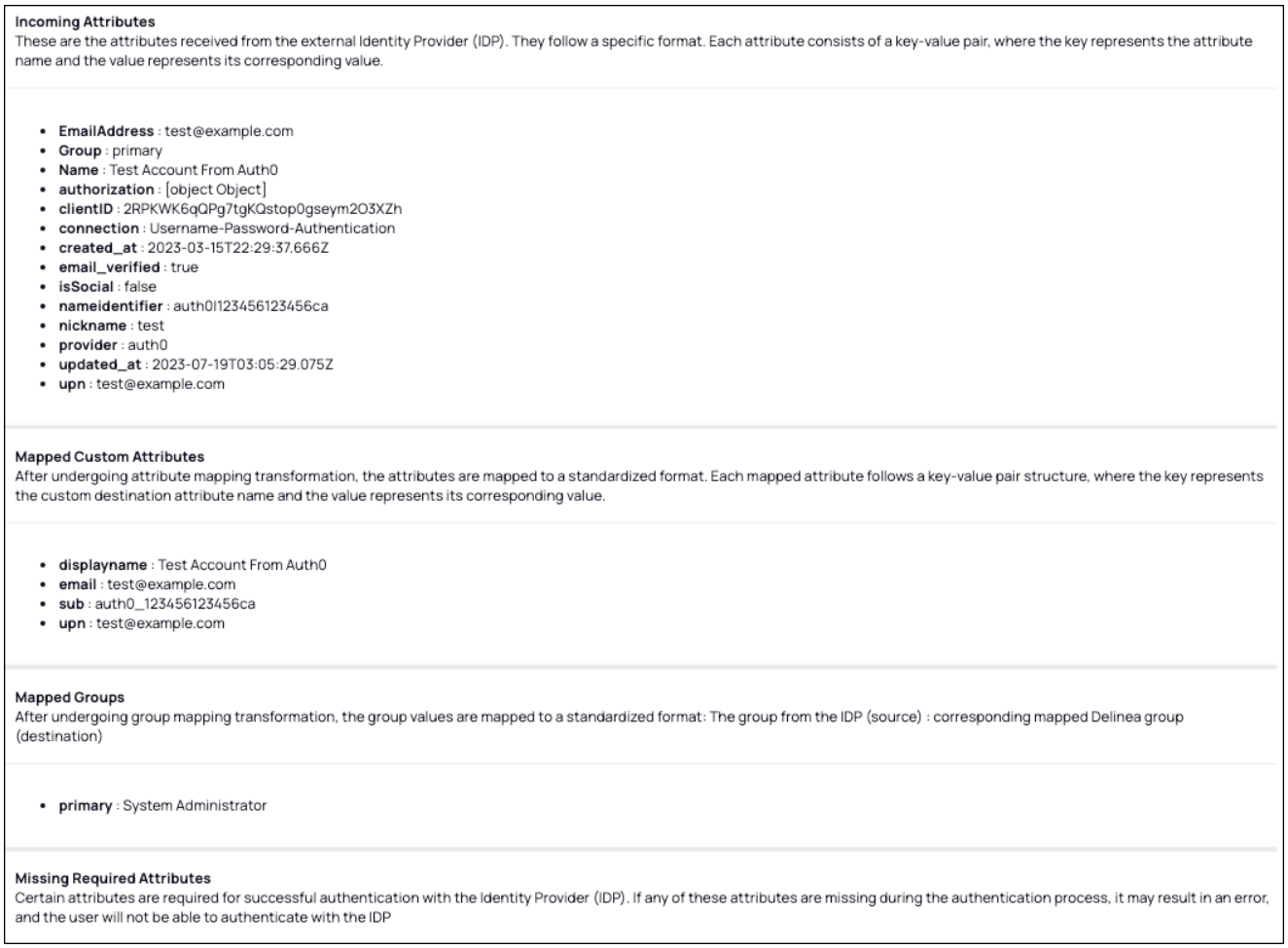
Capturing debug logging is limited to 30 minutes. After that, you need to rerun debugging for continued logging. Logs from previous captures are removed at the end of each duration.

Analyzing Captured Logs

The log collected will provide insights 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 intended to aid in the troubleshooting process

The example below demonstrates a login request by an Auth0 user to the Delinea Platform.



OIDC Flows

Platform federation functionality supports two OIDC flows: Code Flow and Implicit Flow:

Code Flow (Default):

- Applied by default
- Entails an additional step of exchanging an authorization code for tokens
- Strongly recommended due to its superior security features and is suitable for most scenarios

Implicit Flow (Optional):

- Allows clients to directly obtain ID Tokens after authentication
- Not recommended due to its inherent security vulnerabilities

For optimal security and reliability, Delinea recommends using Code Flow by default. Implicit Flow should be used cautiously and only when necessary, considering its potential security risks.

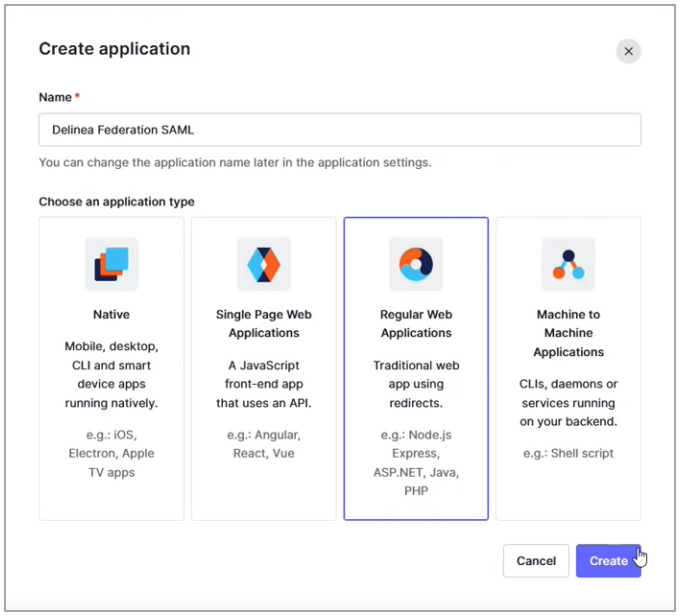
Integrating Auth0

Note: 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.

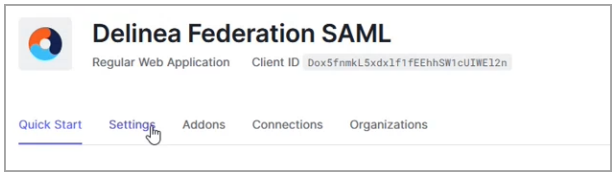
Note: To synchronize newly-federated users and groups, see Federation Management.

Build an Auth0 SAML Application

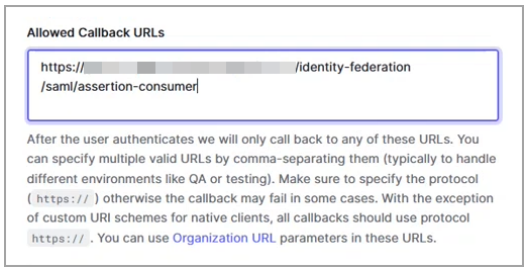
1. From the left navigation menu, click **Applications**.
2. On the Applications page, click **Create Application**.



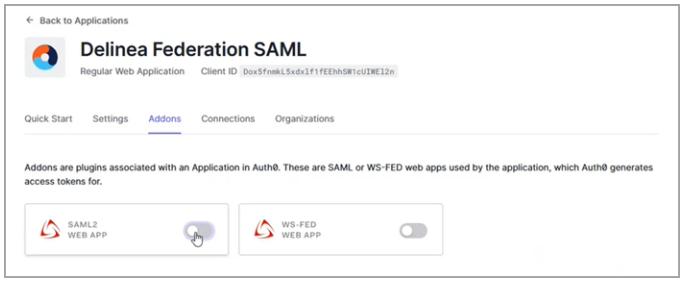
3. On the Create Application page, enter a name for your Auth0 new SAML application, such as `Auth0 SAML`.
4. Choose **Regular Web Applications**.
5. Click **Create**.
6. On your Auth0 new SAML application page, click the **Settings** tab.



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.

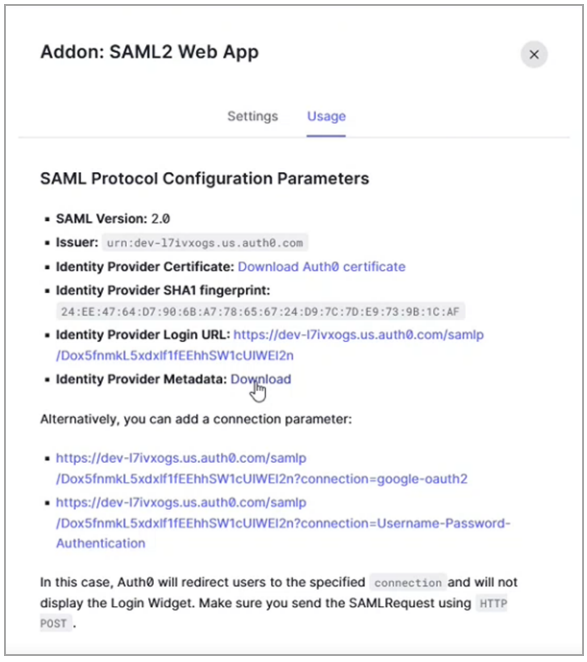


10. Click **Save Changes**.
11. Click the **Add ons** tab.
12. Click the toggle to enable SAML 2.



The **Addon: SAML2 Web App** page opens.

13. 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.

14. Click the **Settings** tab.
15. Scroll to the bottom and click **Enable**.
16. 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 **SAML** from the drop-down menu. The Add Provider page opens.

Add Provider

Create, review, or manage your SAML provider's configuration. Learn more about Federation Settings

Settings

SAML provider configuration: Select file

Name *: Add name

Protocol: SAML

Status: Enabled

Entity ID *: Add entity URL

IDP certificate: Select file

cer, pem or pkcs7 formats are supported

Signature algorithm	None
Thumbprint	Certificate not provided
Not valid before	Certificate not provided
Not valid after	Certificate not provided
Issuer	None

IDP Login URL *: Add URL

IDP Logout URL: Add URL

Platform callback URL: https://example.delinea.app/identity-federation/saml/assertion-consumer

Platform logout URL: https://example.delinea.app/identity-federation/saml/logout-consumer

Advanced Settings

Customize certificate issuer sent to IDP

Force Authentication (ForceAuthN)

Use Login Hint

Request binding: HTTP-Redirect

Sign Request

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	
EmailAddress	email	Required Attribute
Name	displayname	
[illegible]	sub	Required Attribute
upn	upn	Required Attribute

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. **Prompt:** See "Federation Management" on page 52 under Federation Management.
8. **Platform Logout URL**: 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 53 under Federation Management.

Attribute Mappings

See "Attribute Mappings" on page 54 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 "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56 under Federation Management.

Domains

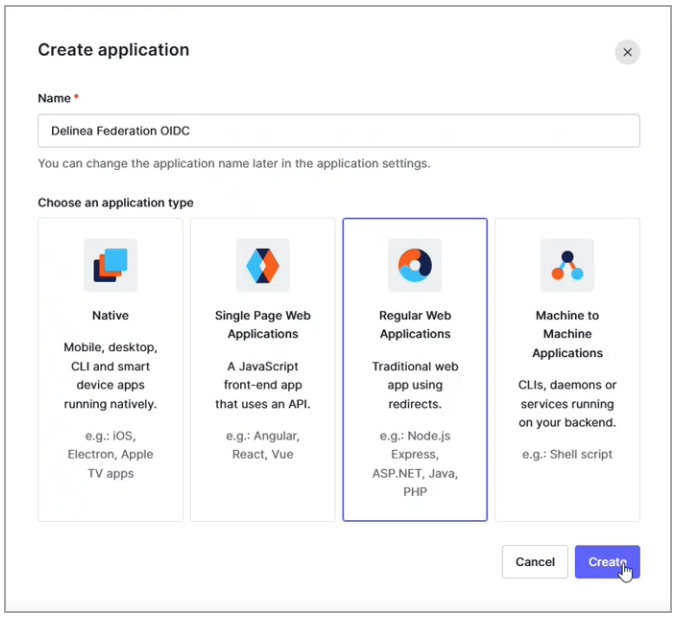
1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.

When all required fields are populated, click **Add Provider**.

Build an Auth0 OIDC Application

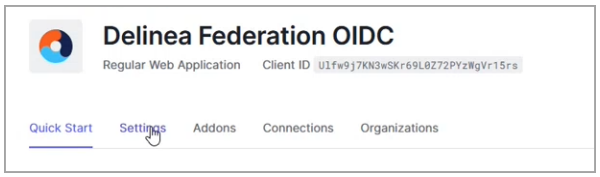
Note: The following procedure requires copying and pasting information between Auth0 and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

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.



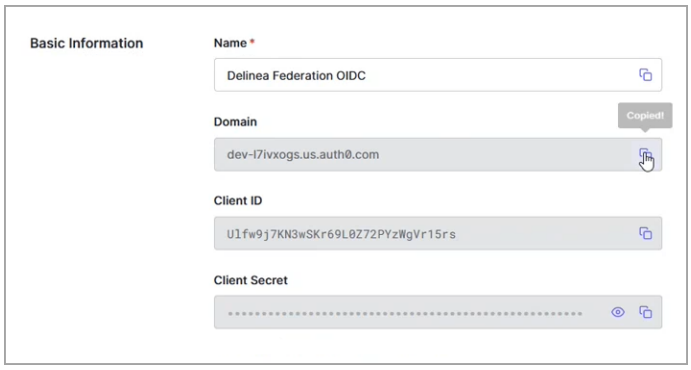
4. Select **Regular Web Applications**.

5. Click **Create**.
6. On your Auth0 new OIDC application page, click the **Settings** tab.



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.



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.

Add Provider

Create, review, or manage your OIDC provider's configuration. Learn more about Federation Settings

Settings

Name *	Add name
Protocol	OIDC
Status	Enabled
Endpoint URL *	Add endpoint URL
Client ID *	Enter client ID
Client secret *	**********
Prompt	Not Specified
Platform callback URL	None

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/nameidentifier	sub	Required Attribute
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	upn	Required Attribute
name	displayname	

Add Attribute Mapping

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME	GROUP

No items found

Add Group Mapping

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	Disabled

Domains

Specify domains users may use as part of their login name

DOMAIN

No items found

Add Domain

Settings

1. **Name**: Enter a unique name.
2. **Status**: Select the box next to **Enabled**.
3. **EndpointURL**: 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. **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 54 under Federation Management.

Group Mappings

Also see "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56 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**.

Integrating Microsoft Entra ID

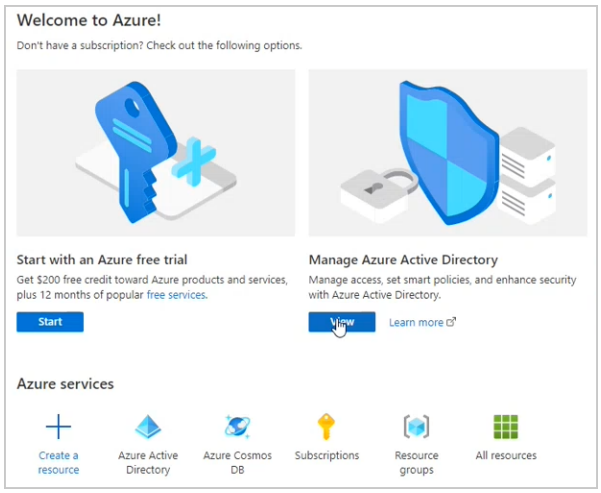
Note: At the end of 2023, Microsoft completed the change of their product name from *Microsoft Azure Active Directory* (Azure AD or ADD) to *Microsoft Entra ID* (Entra or Entra ID).

Note: The following procedures require copying and pasting information between Entra ID and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

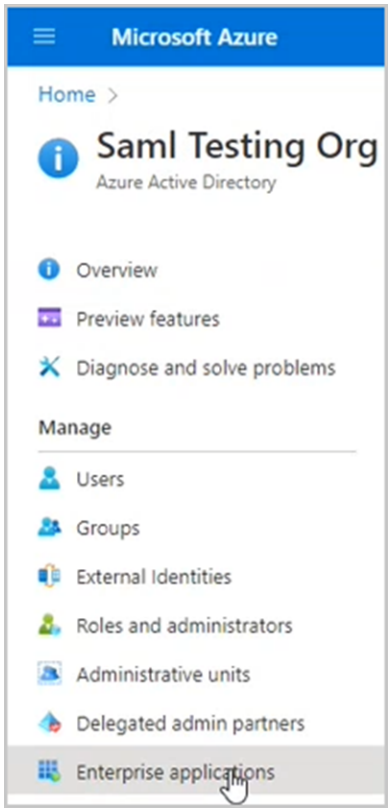
Note: To synchronize newly-federated users and groups, see Federation Management.

Build an Entra SAML Application

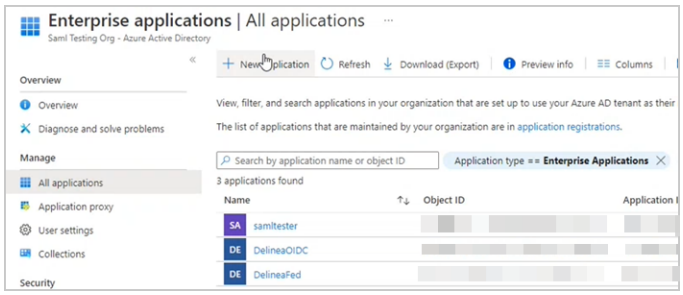
1. Log into the Entra ID portal at `https://entra.microsoft.com`.
2. Click **Manage Entra ID**.



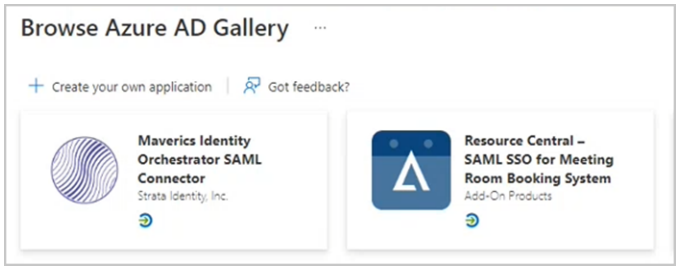
3. From the left panel, click **Enterprise Applications**.



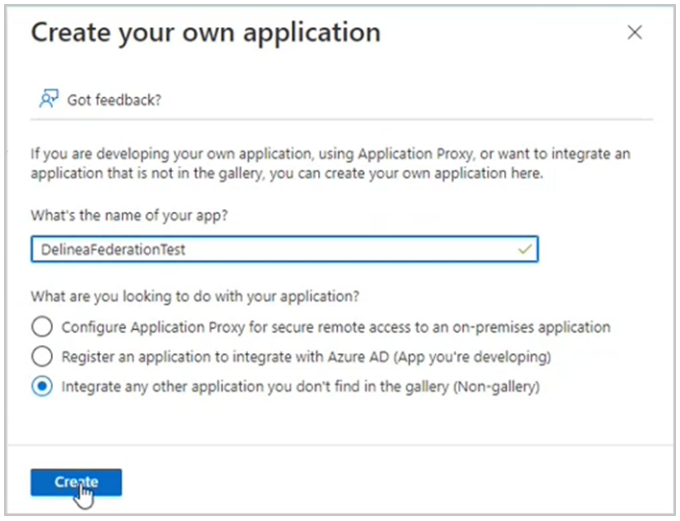
4. From the top row, click **+ New Application**.



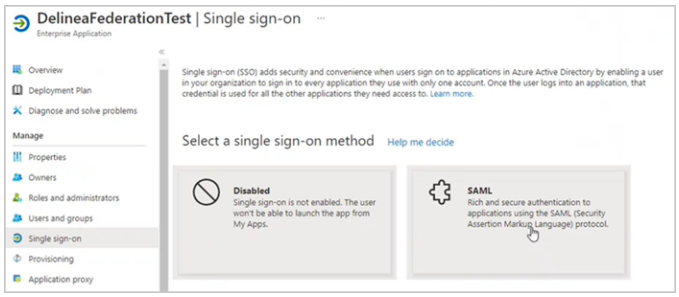
5. At the top of the **Browse Microsoft Entra ID Gallery** page, click **Create your own application**.



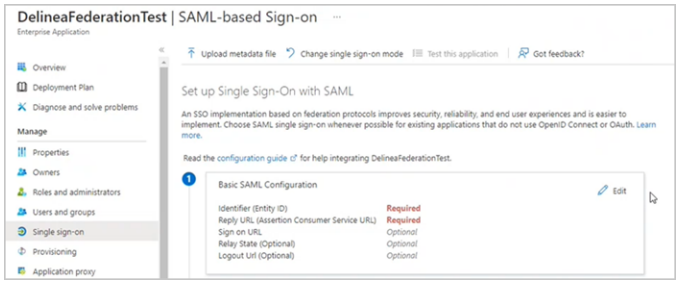
6. On the **Create your own application** page:



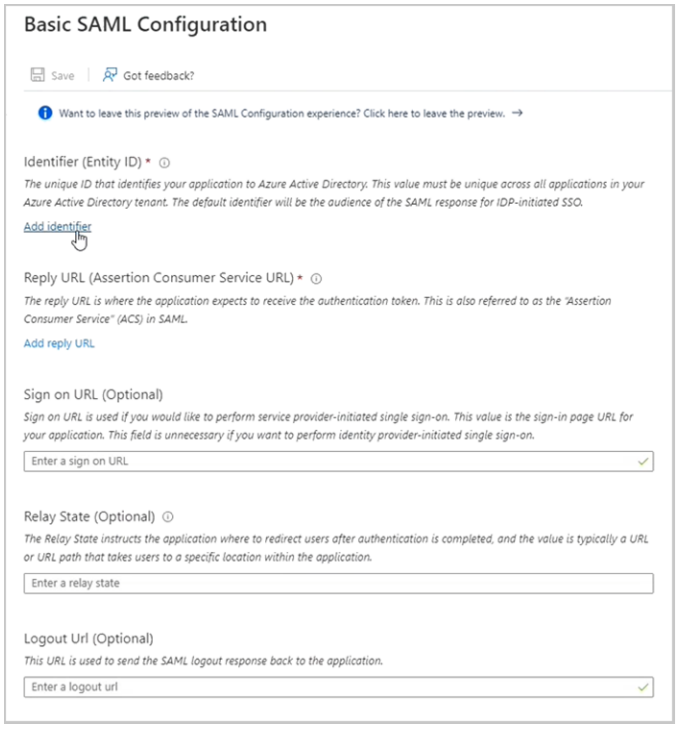
   a. Enter a meaningful name (for example, Delinea Federation).
   b. Ensure this option is selected: **Integrate any other application you don't find in the gallery (Non-gallery)**.
   c. Click **Create**.
7. Once your application is created, click **Single sign-on** from the left panel.
8. Click the SAML card.



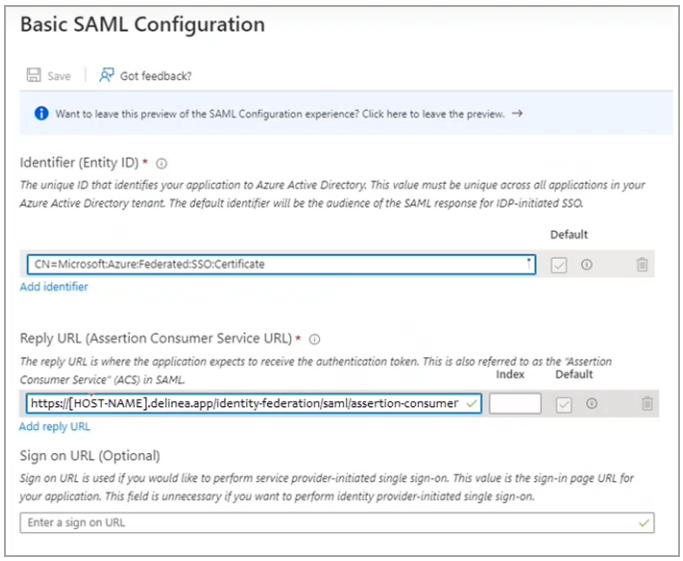
9. On the SAML-based Sign-on page, click **Edit** at the top right of the **Basic SAML Configuration** block



10. In the Basic SAML Configuration panel that appears on the right side, click **Add Identifier**.



11. Add the following values:



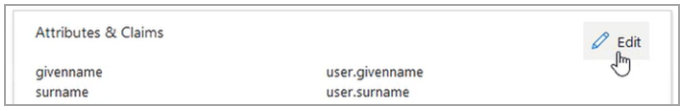
12. **Identity (Entity ID)** `CN=Microsoft:Azure:Federated:SSO:Certificate`
13. **Reply URL (Assertion Consumer Service URL)**
    `https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer`

    Replace `[HOST-NAME]` with the host name you selected when you created your tenant.
14. **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.
15. Click **Save** at the top left.

Attributes and Claims Mappings

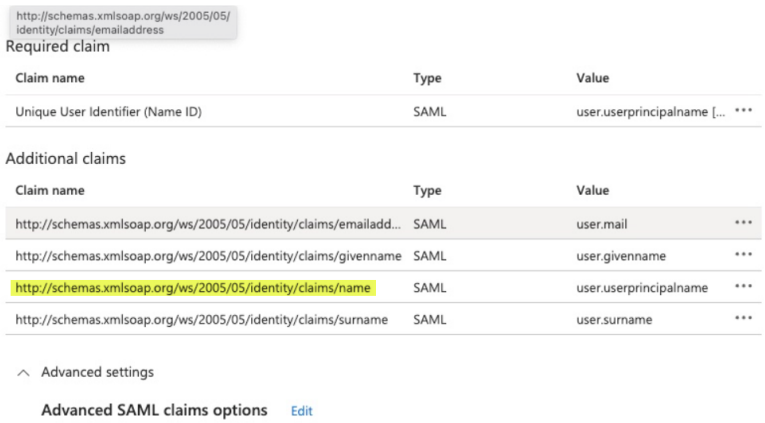
1. Click **Edit** at the right side of the **Attributes & Claims** block.



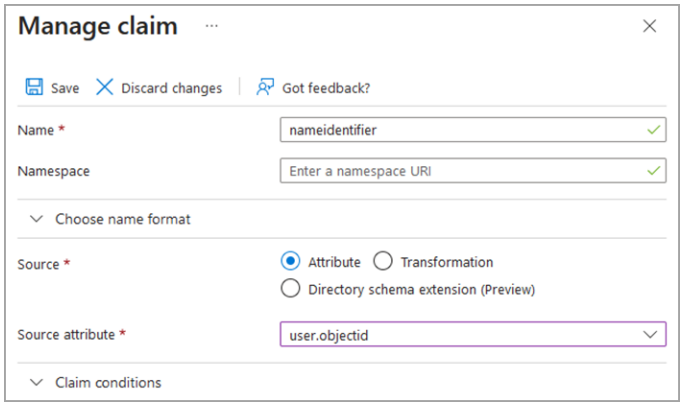
   There are four (4) claims the Delinea Platform requires:

   Source | Destination

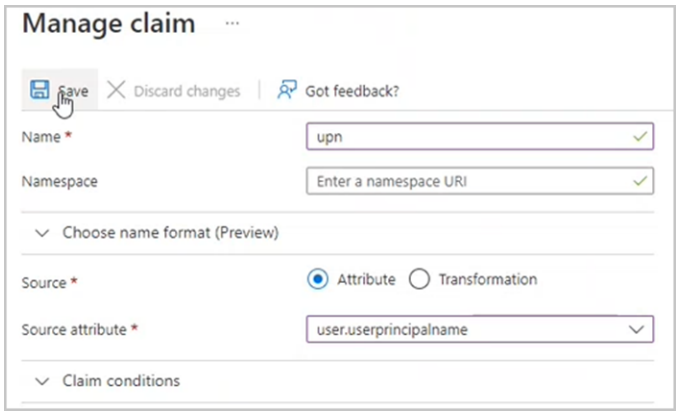
   - EmailAddress | email
   - Name | displayname
   - nameidentifier | sub
   - upn | upn
2. In the **Attributes & Claims** dialog, click the Name claim as shown below and change the Source attribute to `user.displayname`.



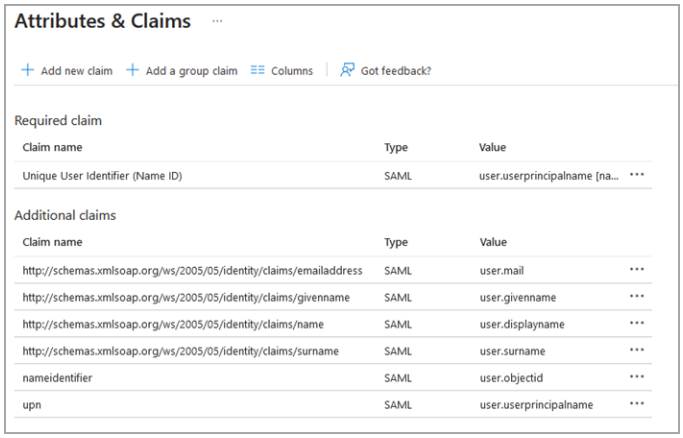
3. Click **Save**.
4. Click **Add new claim**.
5. On the **Manage Claim** page, enter the following values:
   - **Name:** `nameidentifier`
   - **Source Attribute:** `user.objectid`



6. Click **Save**.
7. Add a second claim for the for upn using the following values:
   - **Name**: `upn`
   - **Source Attribute**: `user.userprincipalname`

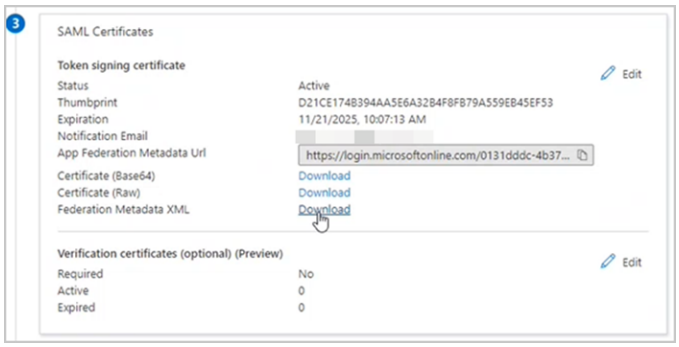


8. Click **Save**. Your final claims appear.



9. Click the **SAML-based Sign-on** link to go back to the SAML setup screen.

10. In the **SAML Certificates** block, click **Download** next to **Federation Metadata XML** and **Certificate (Base64)**



You will use these saved files in the next step to configure the Federation service in your Delinea tenant.

Add the Provider to the Platform

1. Log back 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.

Add Provider

Create, review, or manage your SAML provider's configuration. Learn more about Federation Settings

Settings

SAML provider configuration: Select file

Name *: Add name

Protocol: SAML

Status: Enabled

Entity ID *: Add entity URL

IDP certificate: Select file

cer, pem or pkcs7 formats are supported

Signature algorithm	None
Thumbprint	Certificate not provided
Not valid before	Certificate not provided
Not valid after	Certificate not provided
Issuer	None

IDP Login URL *: Add URL

IDP Logout URL: Add URL

Platform callback URL: https://example.delinea.app/identity-federation/saml/assertion-consumer

Platform logout URL: https://example.delinea.app/identity-federation/saml/logout-consumer

Advanced Settings

Customize certificate issuer sent to IDP

Force Authentication (ForceAuthN)

Use Login Hint

Request binding: HTTP-Redirect

Sign Request

Attribute Mappings

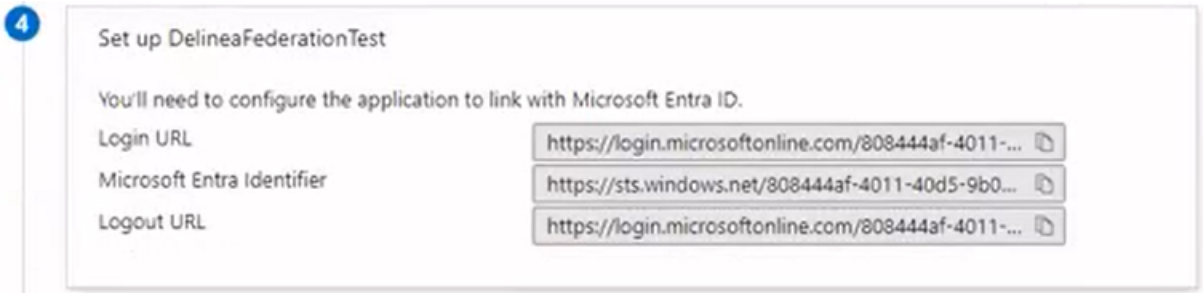
User attributes that are passed from the identity provider (IdP) to the Delinea Platform (SP) during the authentication and authorization process

SOURCE	DESTINATION	
EmailAddress	email	Required Attribute
Name	displayname	
nameidentifier	sub	Required Attribute

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.



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
   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
8. **Status**: Select the box next to Enabled.

Advanced Settings

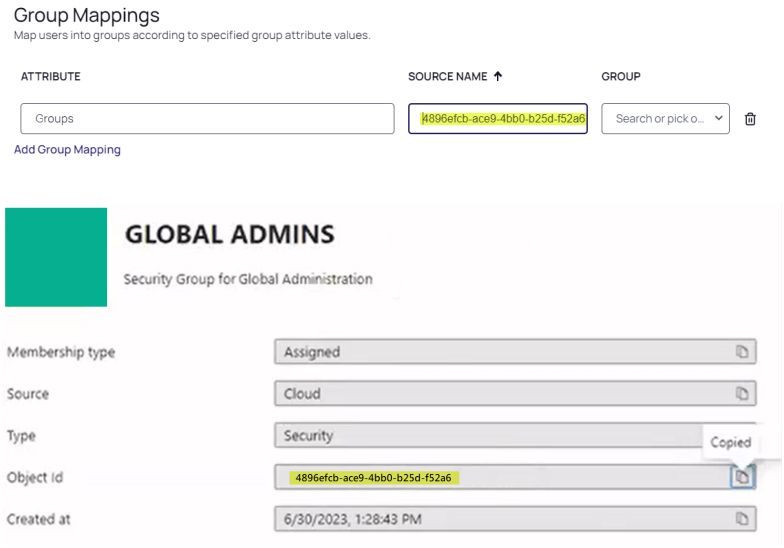
See "Advanced Settings (SAML only)" on page 53 under Federation Management.

Attribute Mappings

- EmailAddress | email
- Name | displayname
- nameidentifier | sub
- upn | upn

Group Mappings

1. Click **Add Group Mapping**.
2. Under **Attribute**, enter 'groups'.
3. Under **Source Name**, enter the **Object ID** (highlighted in both images below) copied from the appropriate group on the Microsoft Entra ID Groups page.



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 "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56.

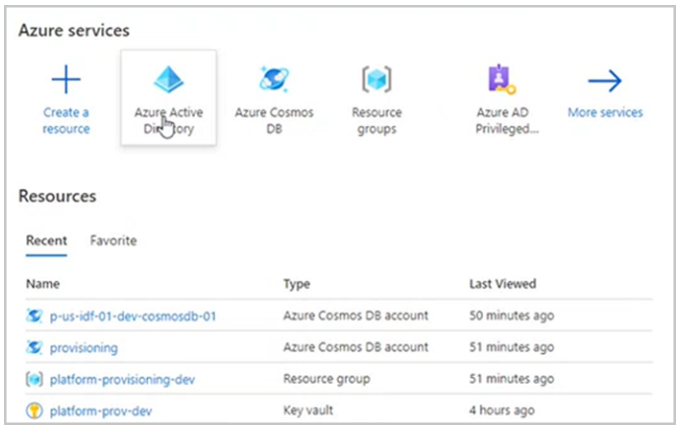
Domains

1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.

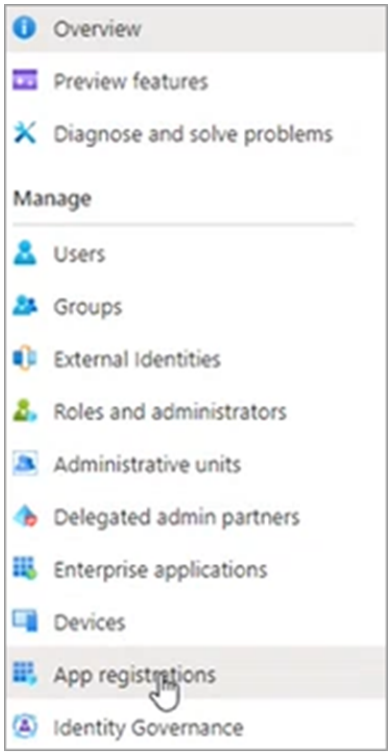
When all required fields are populated, click **Add Provider**.

Build an Entra OIDC Application

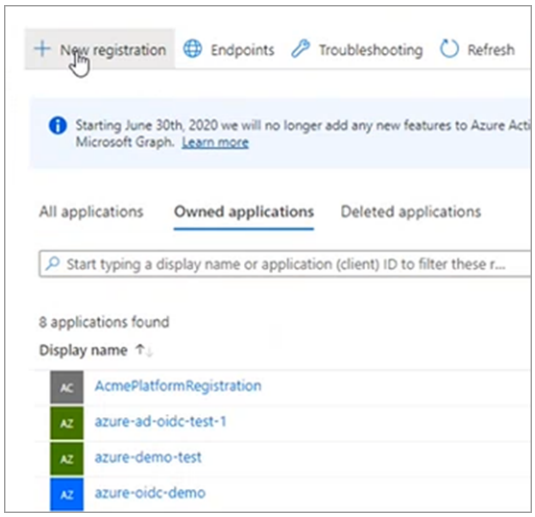
1. Log into the Entra ID portal.
2. From the Entra ID Home page, click the **Entra ID** icon.



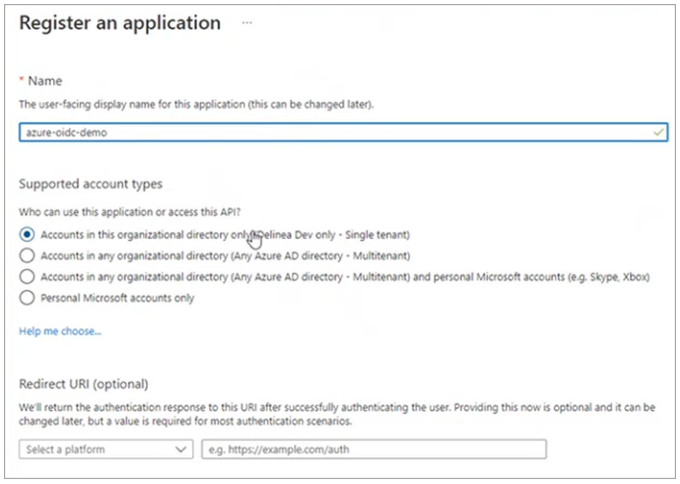
3. Once inside the Entra ID service, click **App Registrations** from the left navigation.



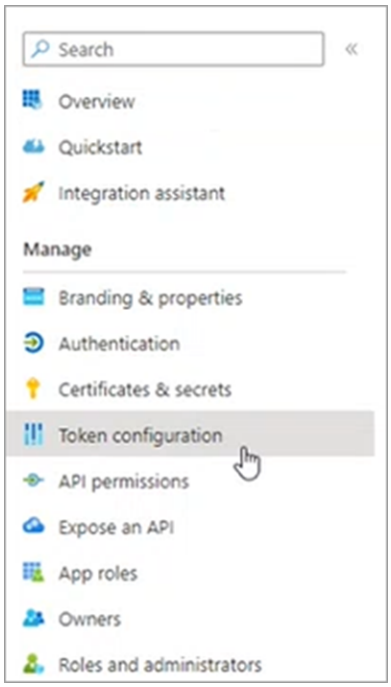
4. Along the top row, click **+ New Registration**.



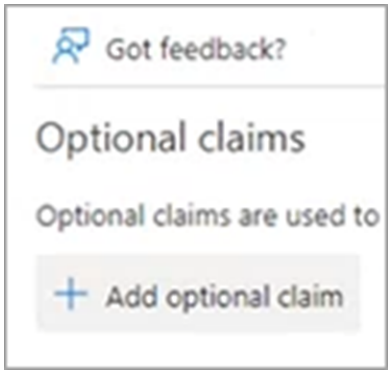
The **Register an application** page appears.



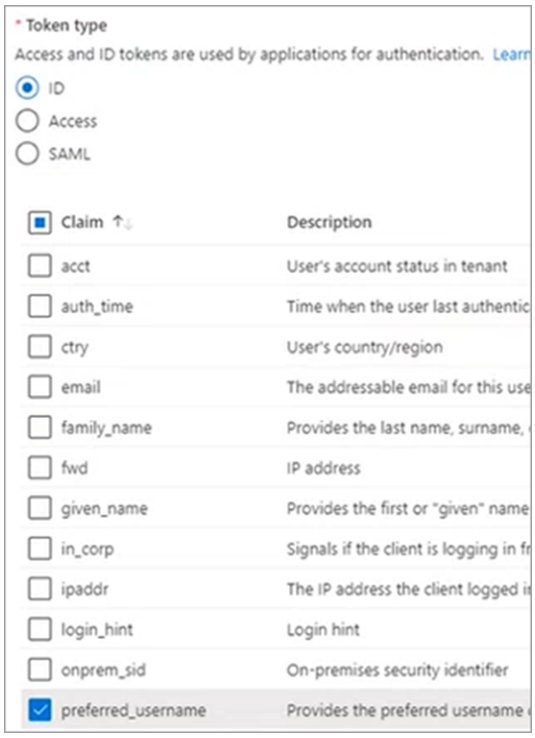
5. Fill out the fields as follows:
   - **Name**: Give the new application you are registering a name. Any descriptive name works. This name will be displayed to users by Microsoft during the first login but it does not matter to the Delinea Platform. For demonstration purposes, we will use the name `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 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.

4. The Add Provider page opens.

Add Provider

Create, review, or manage your OIDC provider's configuration. Learn more about Federation Settings

Settings

Name *	Add name
Protocol	OIDC
Status	Enabled
Endpoint URL *	Add endpoint URL
Client ID *	Enter client ID
Client secret *	**********
Prompt	Not Specified
Platform callback URL	None

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/nameidentifier	sub	Required Attribute
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	upn	Required Attribute
name	displayname	

Add Attribute Mapping

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME	GROUP

No items found

Add Group Mapping

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	Disabled

Domains

Specify domains users may use as part of their login name

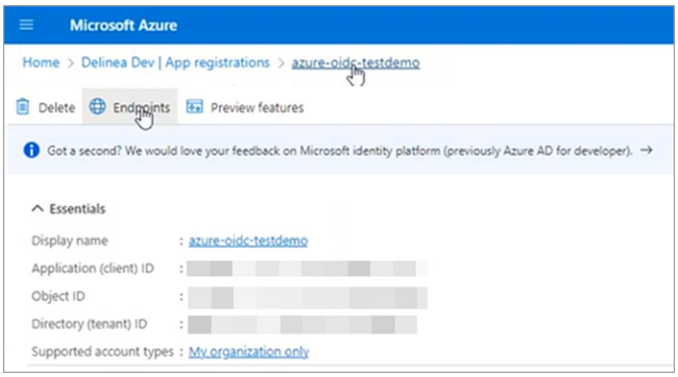
DOMAIN

No items found

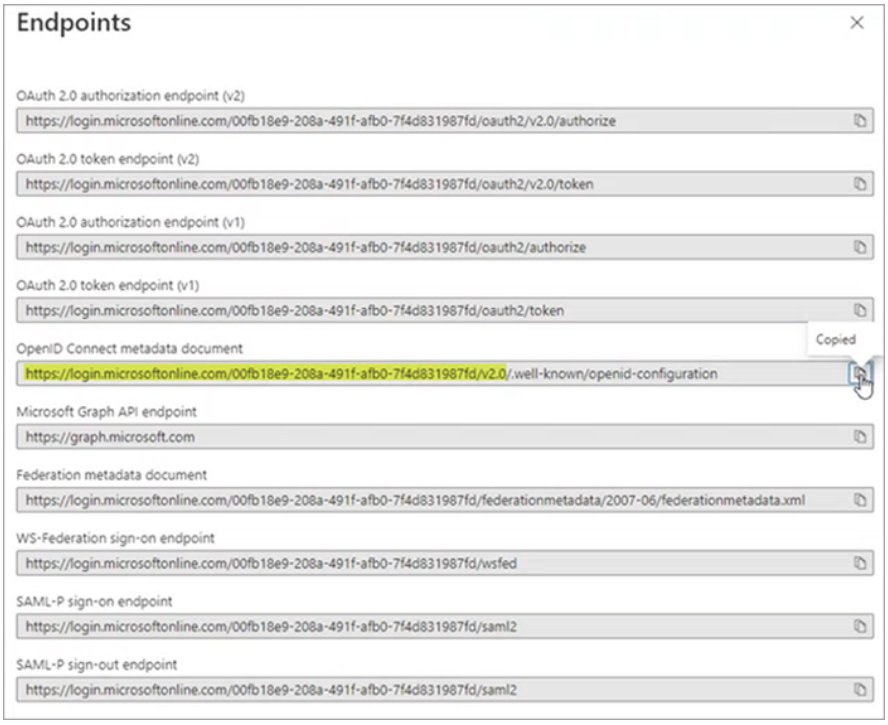
Add Domain

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 Azure app 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 Azure app 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 "Federation Management" on page 52 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.

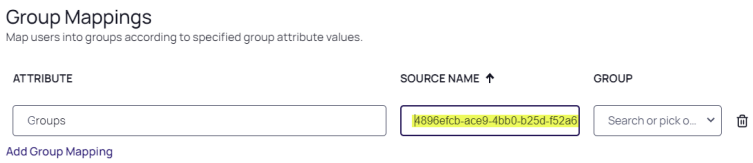
Attribute Mappings

Some defaults are provided but can be overridden as needed. In this example we will replace the upn value with preferred_username.

- 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 **Group**.
3. Under **Source Name**, enter the **Object ID** (highlighted in both images below) copied from the appropriate *groups* on the Microsoft Entra ID Groups page.



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 "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56 under Federation Management.

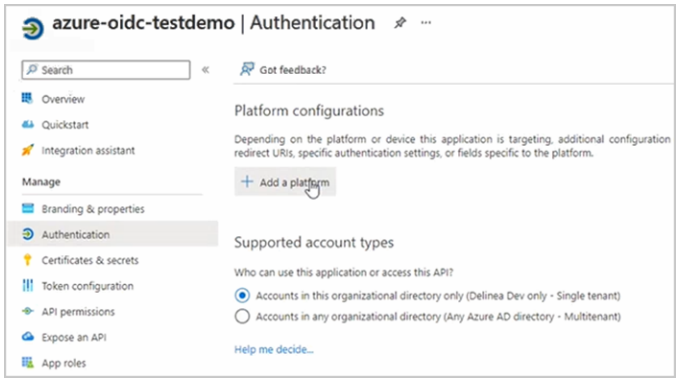
Domains

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**.

Add the Platform

1. On the **Entra App Registration** page, click **Authentication** and then **Add a platform**.

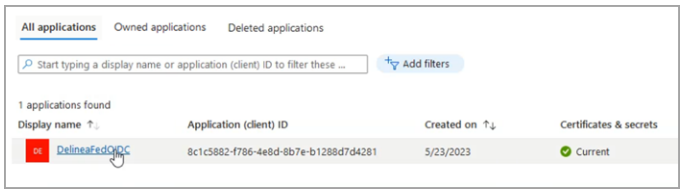


2. In the panel that opens on the right, click **Web**.

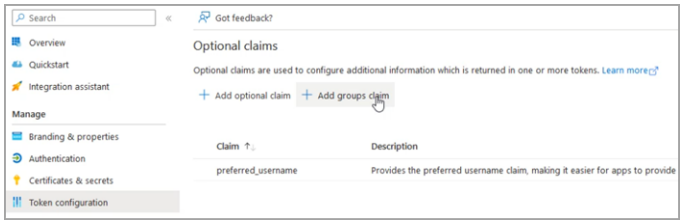
3. Under **Redirect URIs**, enter your Platform Callback URL from your provider page.
4. Click **Configure** at the bottom of the panel.

From Your Entra Application

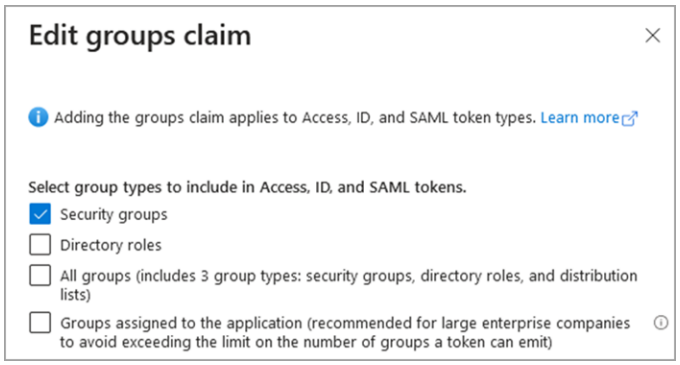
1. Log in to your Microsoft Entra ID application and open to the Home page.
2. From the left navigation menu, click **App Registrations**.
3. Click the **All applications** tab.
4. Click the appropriate SAML or OIDC federation application created by your organization, for example:



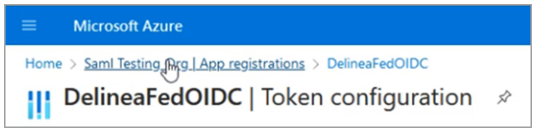
5. From the left menu navigation, click **Token Configuration**.



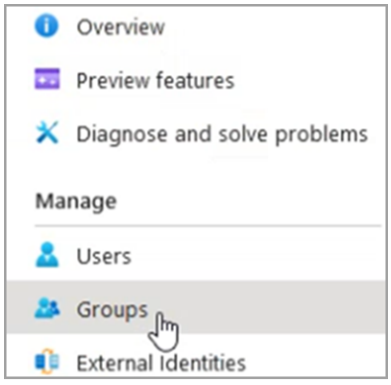
6. Click **+ Add group claim**.
7. From the panel that pops up named **Edit group claims**, select the group types to include. We strongly recommend selecting **Groups assigned to the application** to ensure that only the needed groups are sent to the platform.



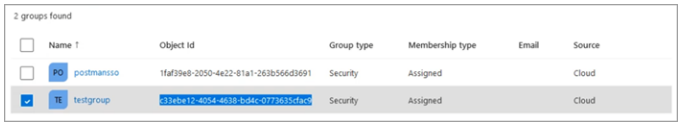
8. Click **Add** at the bottom.
9. From the breadcrumb path at the top of the page, select the name of the Entra ID directory you're configuring, for example:



10. Click **Groups** from the left navigation menu.



11. Select the group you are working with and copy the group's Object ID.



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.

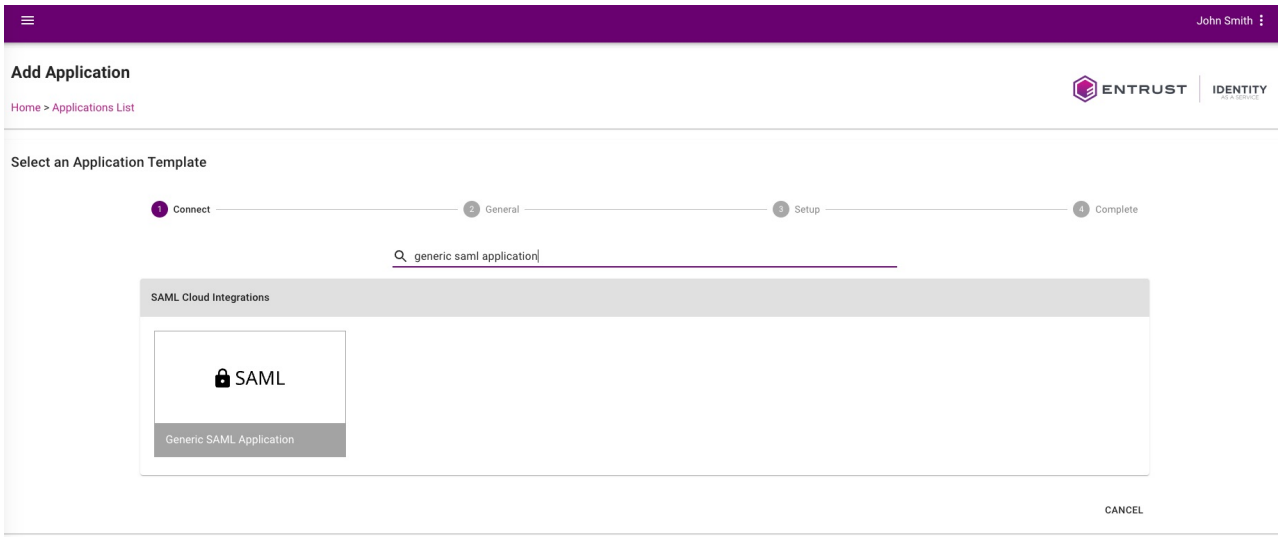
5. Click the **Members** tab.
6. Verify that the user you logged in as, is a member of the platform group that you mapped to an Microsoft Entra ID group.

Integrating Entrust

> On the Delinea Platform, you need admin with federation privileges.
>
> In Entrust, you need admin access to create SAML and OIDC applications.
>
> The following procedures require copying and pasting information between Entrust and the Delinea Platform. We recommend opening both applications in separate browser windows.

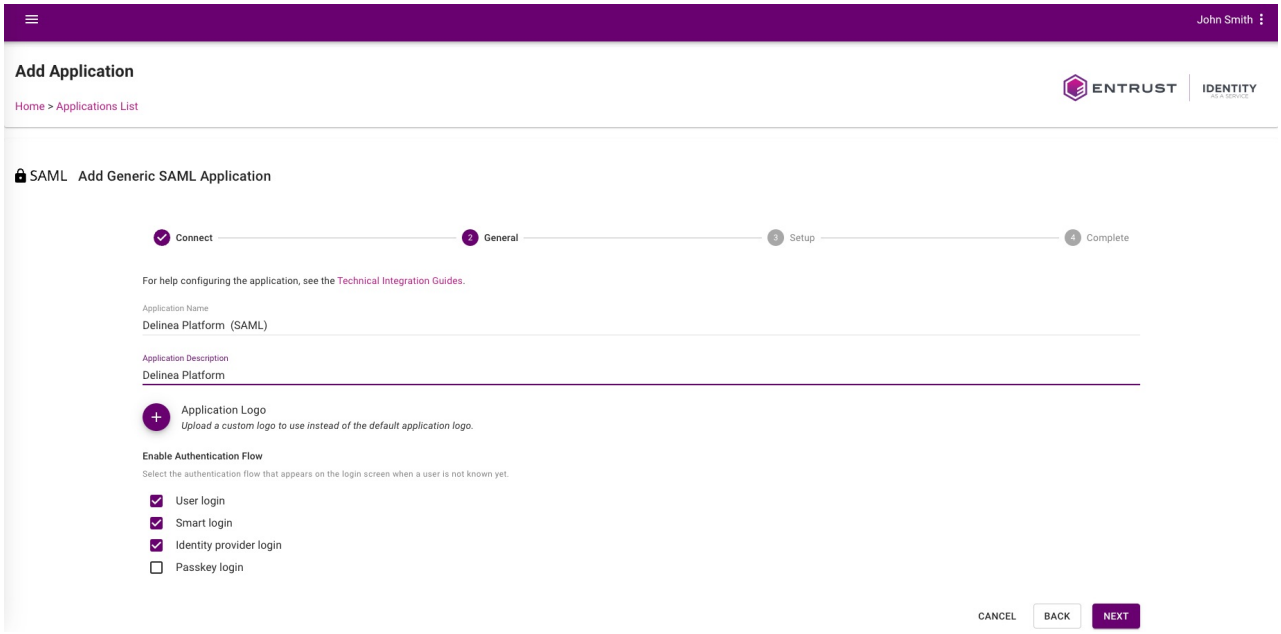
Build an Entrust SAML Application

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.**

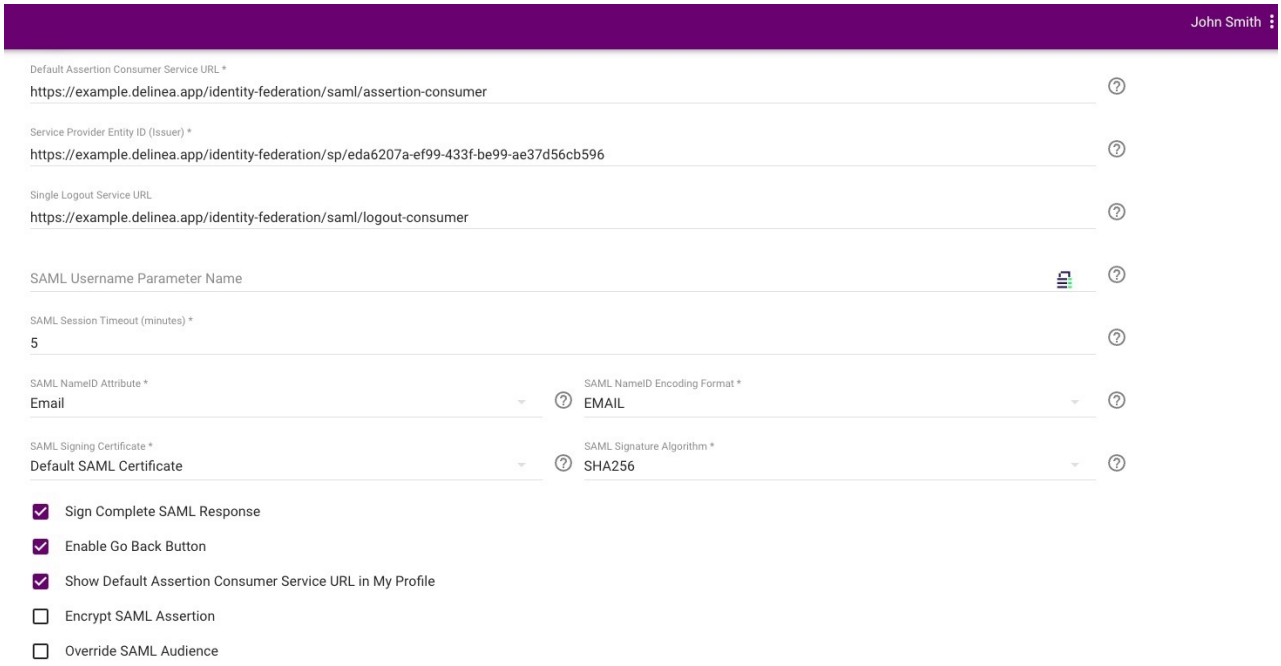


7. In the next section **General**, apply the following settings.

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 https://[HOST-NAME].delinea.app/identity-federation/sp/undefined *The value, “undefined”, is temporary and will be replaced with a GUID value later.
Single Logout Service URL	Platform logout URL https://[HOST-NAME].delinea.app/identity-federation/saml/logout-consumer

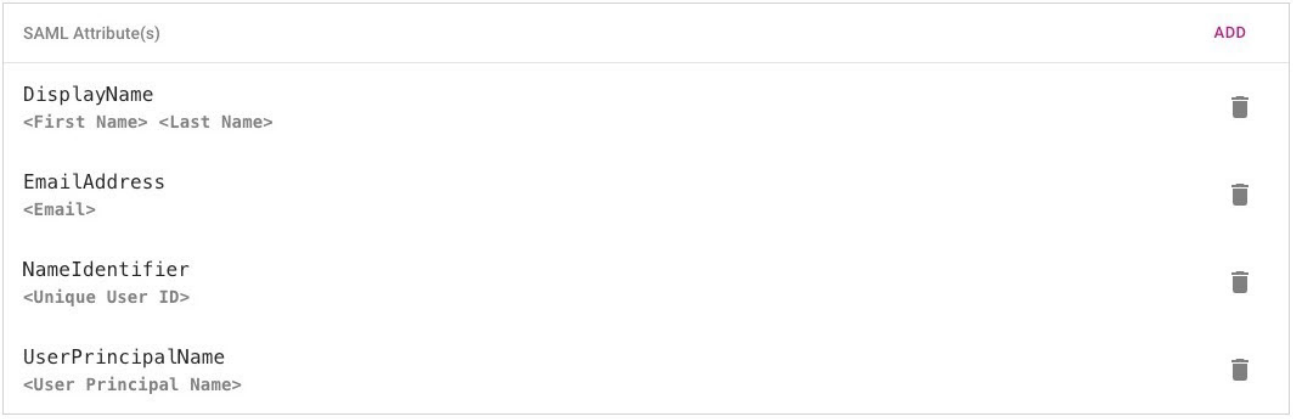
8. Continue updating the following application settings by selecting the value from the drop-down menu.

Entrust setting	Value
SAML NameID Attribute	Email
SAML Signing Certificate	`Default SAML Certificate` or you may specify another one
SAML NameID Encording Format	EMAIL
SAML Signature Algorithm	SHA256

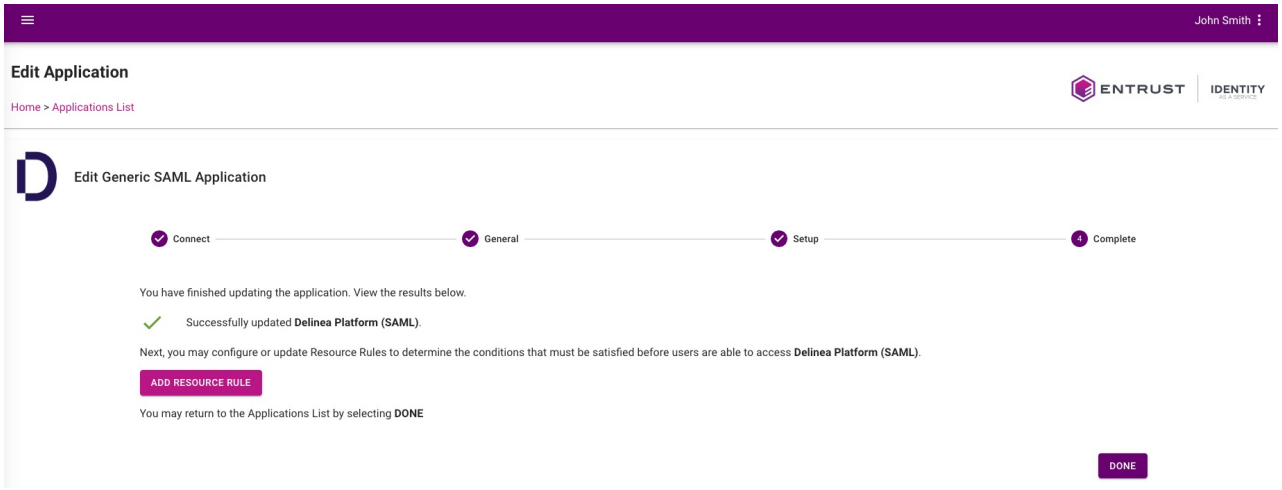


9. Add SAML Attribute(s) with the key value pairs and click **Submit**.

Name	Value
DisplayName	<First Name> <Last Name>
EmailAddress	<Email>
NameIdentifier	<Unique User ID>
UserPrincipalName	<User Principal Name>



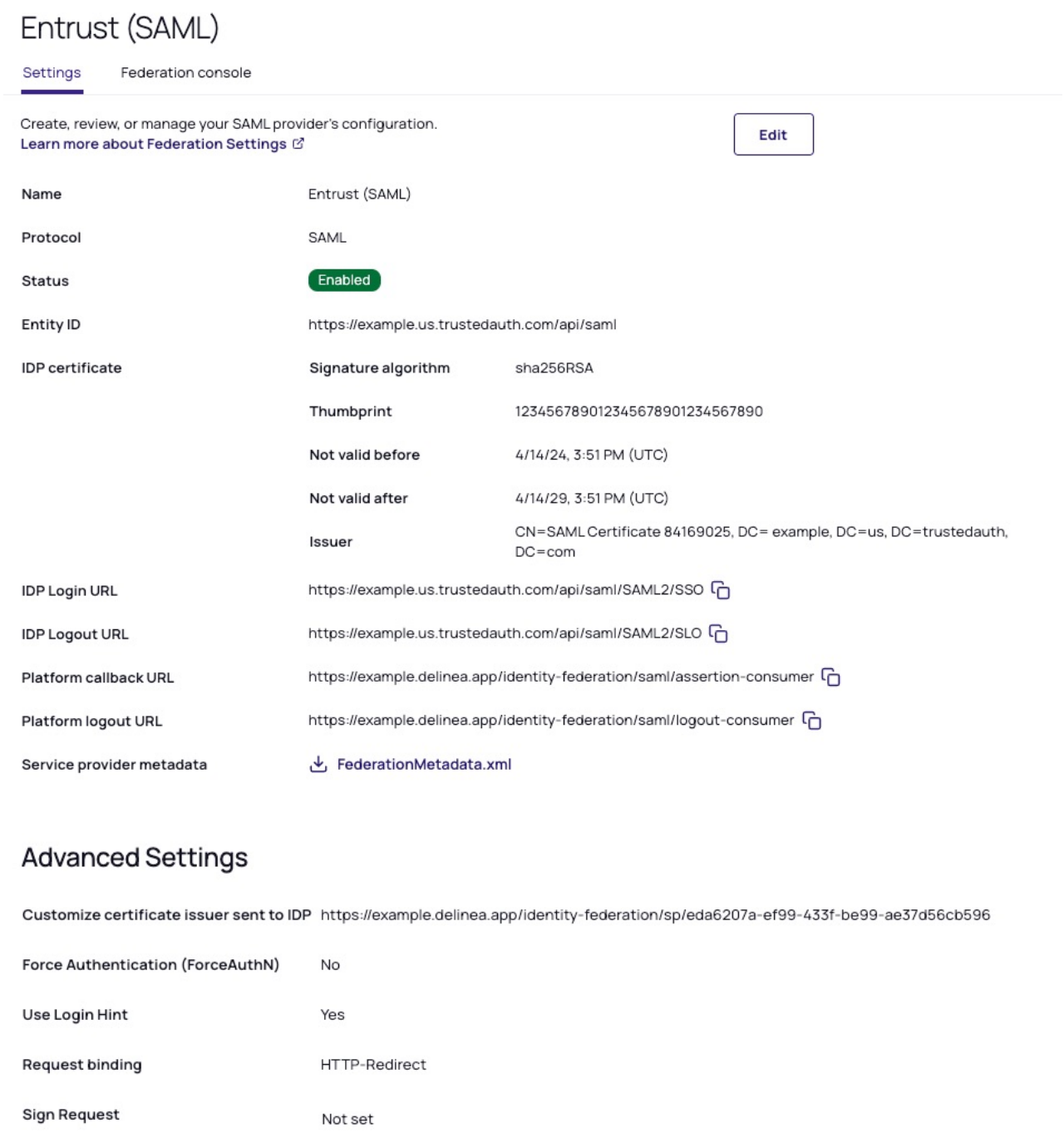
10. Configure or update **Resource Rules** to specify the conditions users must meet to access the newly created application.



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 Delinea Platform.

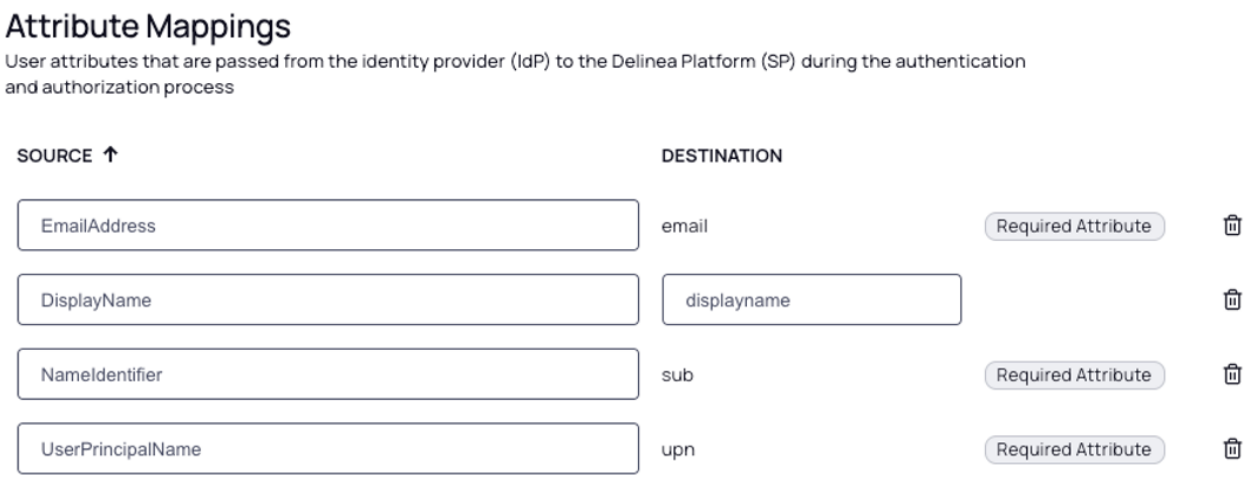
Add a Delinea Platform SAML Provider

1. Log in to the Delinea Platform.
2. Navigate to **Settings** > **Federation Providers**.
3. Click **Add Providers** and create a SAML provider.
4. Under **Settings** click **Select file** and upload the SAML IDP metadata file previously downloaded from Entrust and click **Apply**. This step will also save the provider.
5. Click **Edit** to update the SAML provider configuration.
6. Update the **Name** field with a unique name for the provider.
7. Enable **Customize certificate issuer sent to IDP**.
8. Copy the value and paste it in the **Service Provider Entity ID** field in the SAML application on Entrust.



9. Update the Attribute Mappings as follows:

Source	Destination
EmailAddress	email
DisplayName	displayname
NameIdentifier	sub
UserPrincipalName	upn

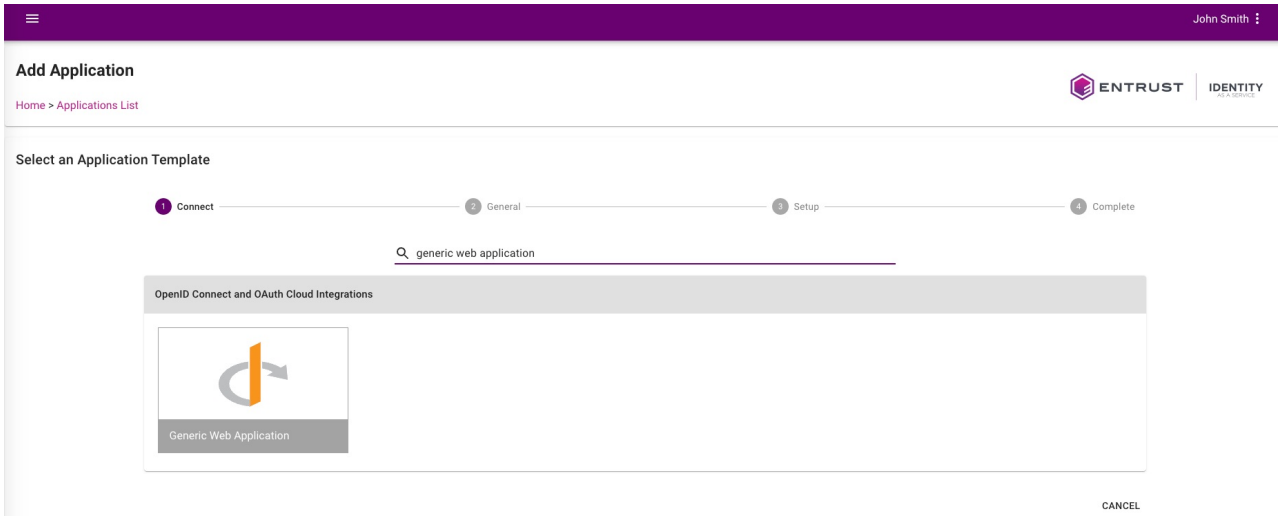


10. Click **Add Domain** to add your domain(s).
11. Optionally set the status to **Enabled**.
12. **Save** settings.

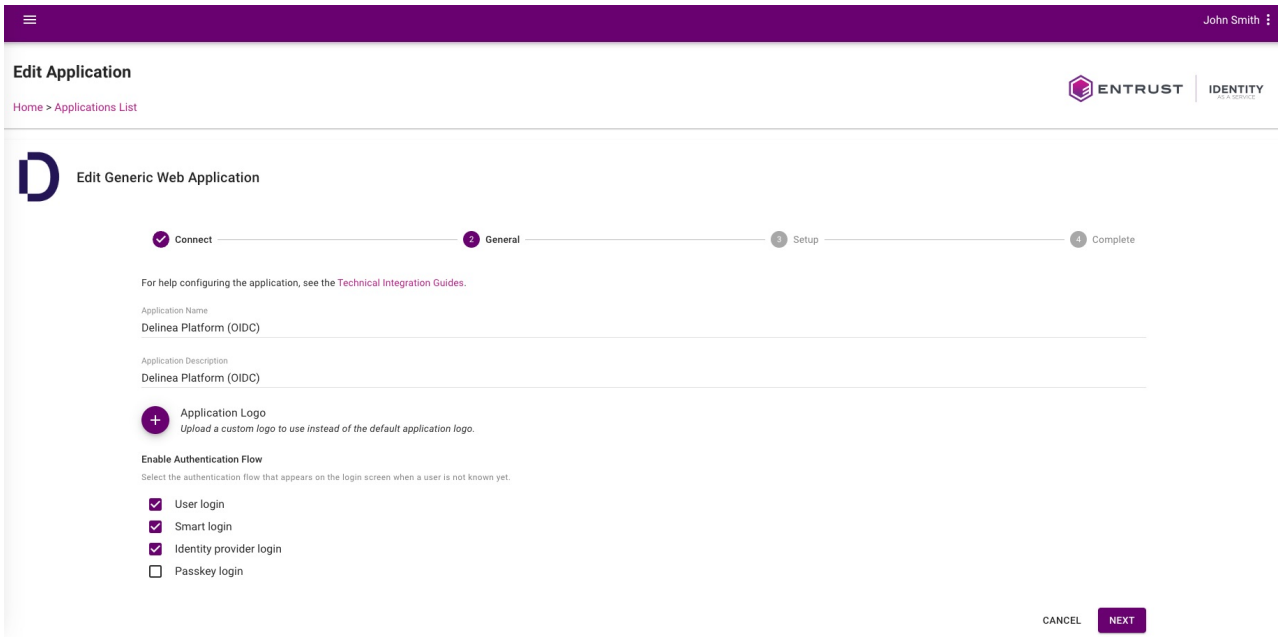
Build an Entrust OIDC Application

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**.

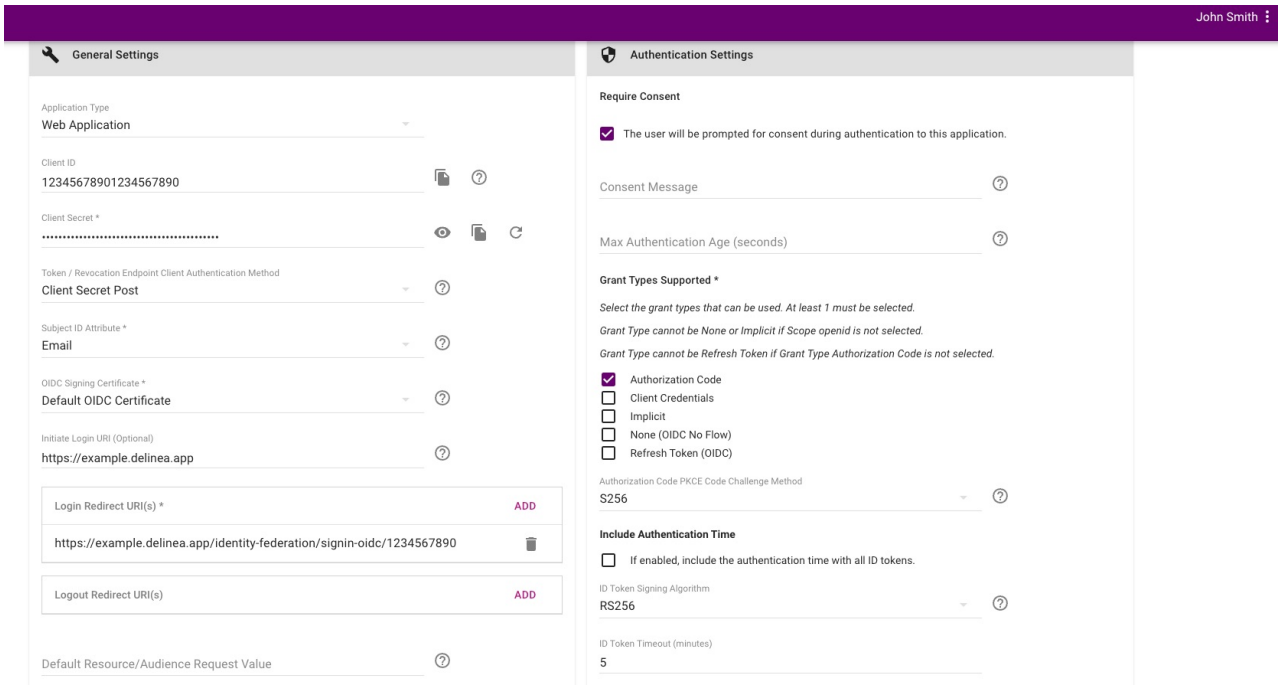


5. Provide a unique **Application Name**.
   - Optionally, provide a logo for the application, and a description.
6. Click **Next**.



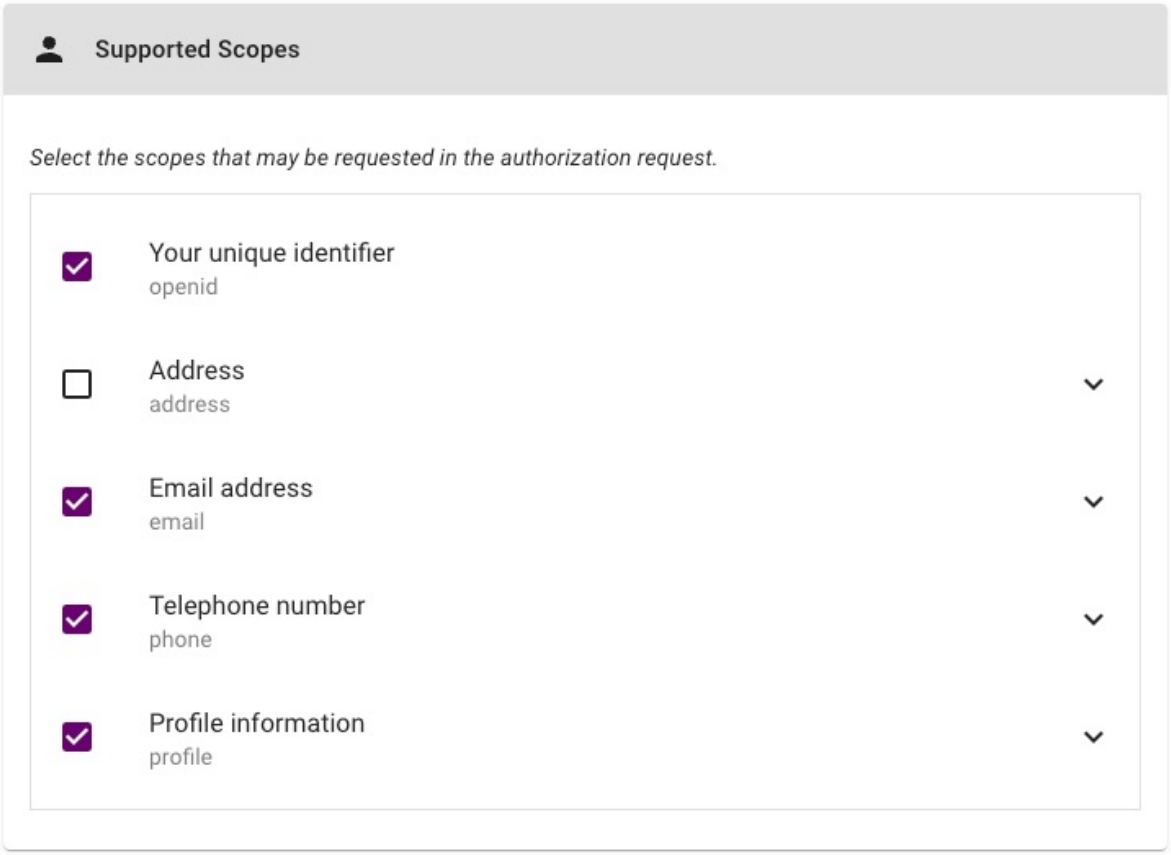
7. Under the next section **General**, apply the following settings:

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 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



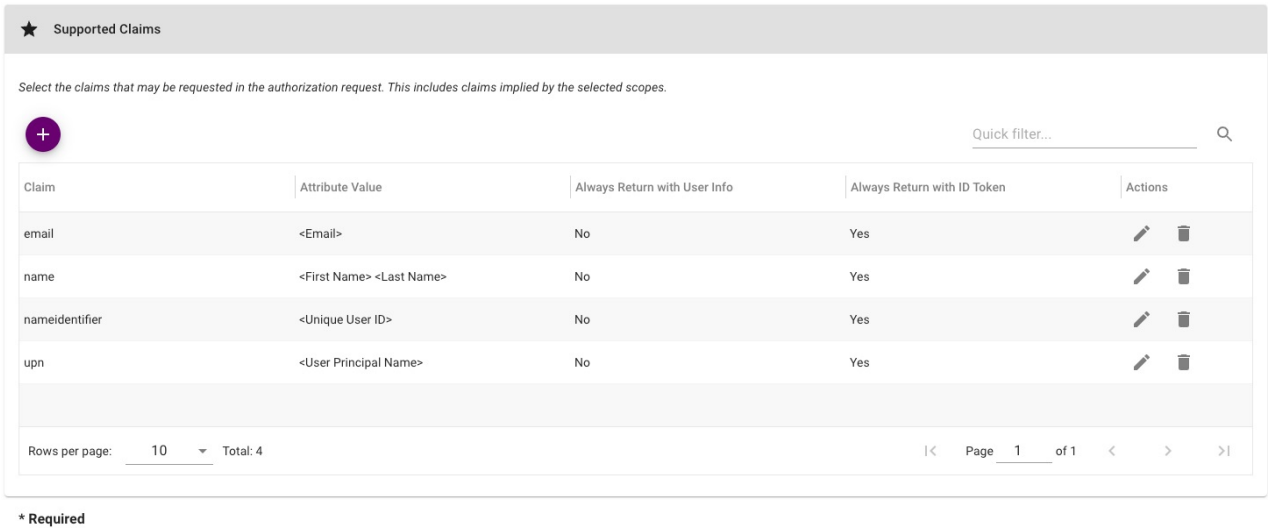
8. Ensure that you select the following application support scopes:
   - Your unique identifier
   - Email address
   - Telephone number (optional)

- Profile information

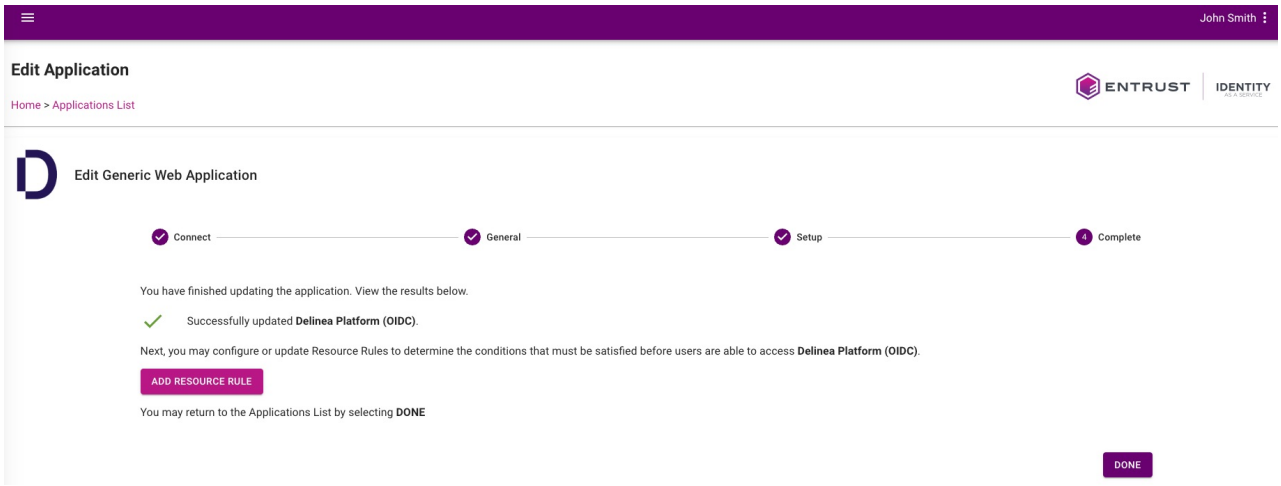


9. Next, add or update the supported claims and ensure that they are always returned with ID Token.

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



10. Click **Submit**.
11. Configure or update **Resource Rules** to specify the conditions users must meet to access the newly created application.

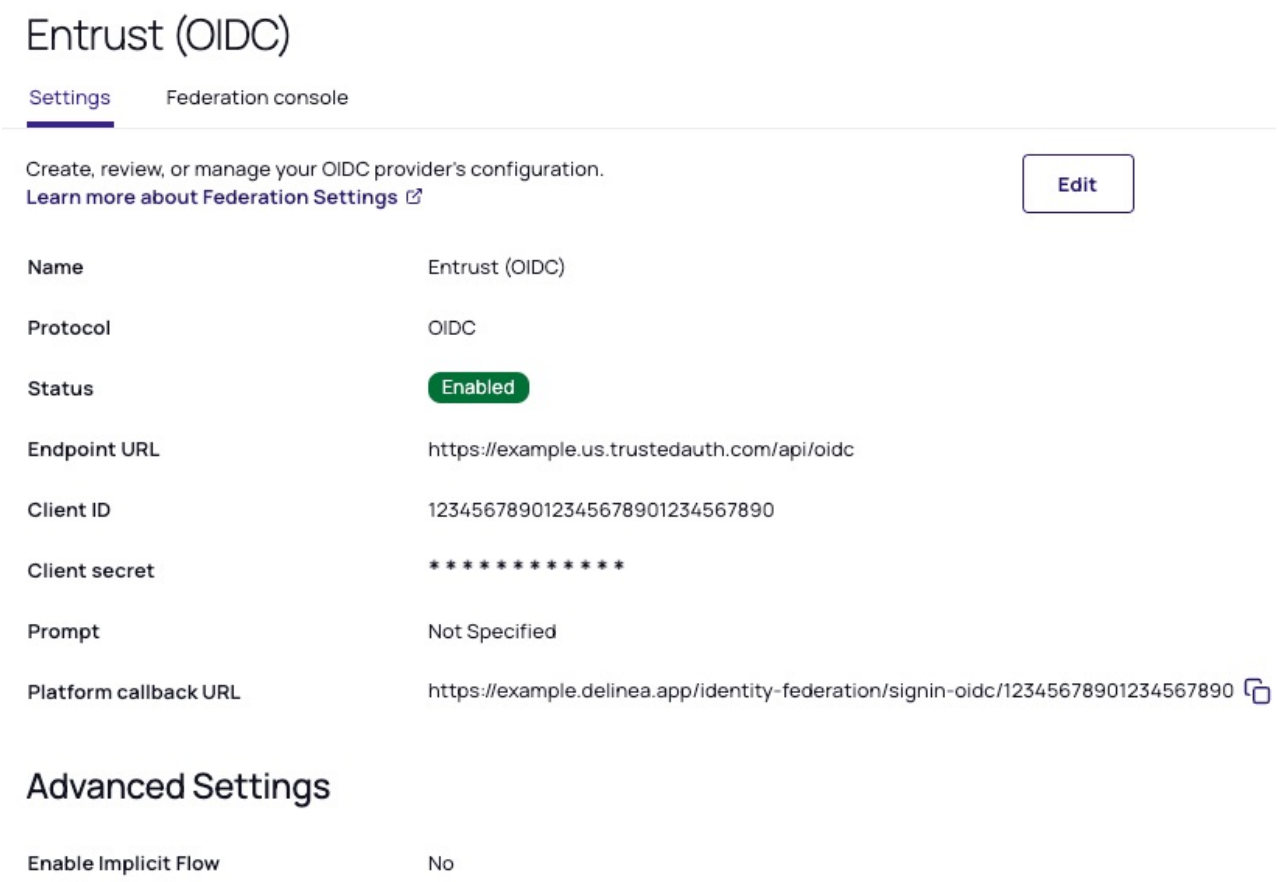


12. Click **Submit** when you are finished configuring your Resource Rules.

Add a Delinea Platform OIDC Provider

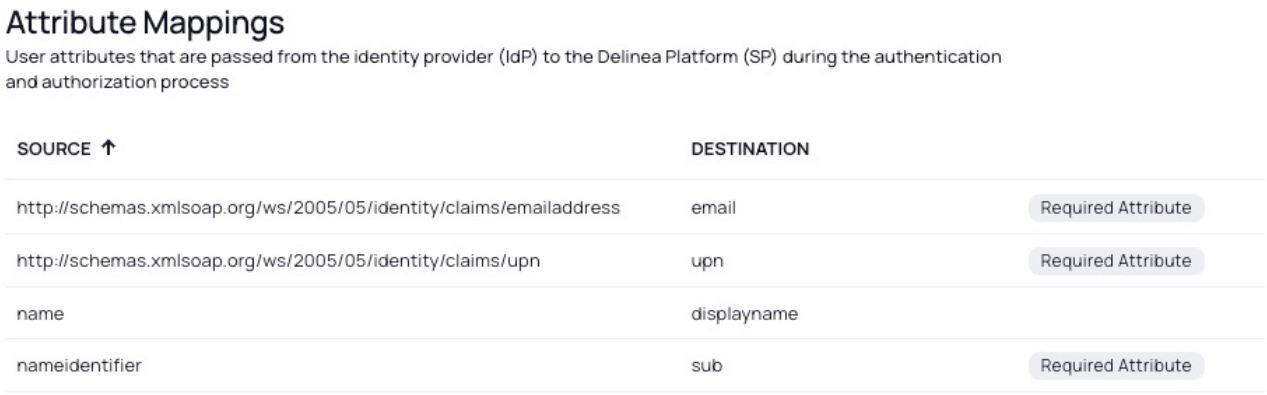
1. Navigate to **Settings** > **Federation Providers**.
2. Create a new OIDC provider.
3. Provide a unique name for your provider (e.g. Entrust - OIDC).
4. Update these settings:

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



5. Save your settings.
6. Re-edit the OIDC provider just created in platform.
7. Make note of the **Platform Callback URL** as this is needed in your Entrust application.
8. Update these 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



9. Add your domain(s).
10. Enable the status of the provider.
11. Save your settings.

Test Configuration

Before testing, make sure you address the following:

- Be sure that you have a 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 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.

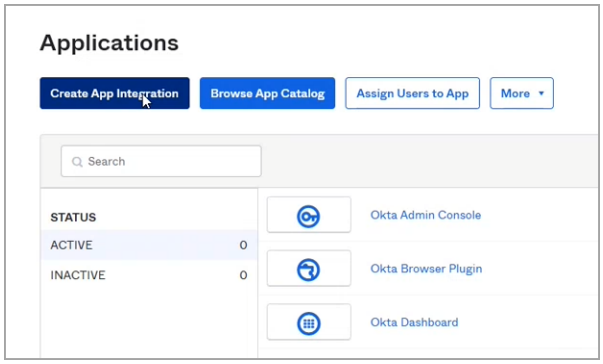
Integrating Okta

Note: To synchronize newly-federated users and groups, see Federation Management.

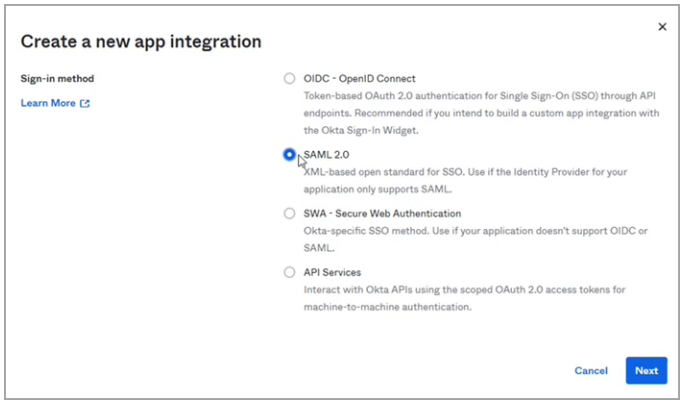
Note: The following procedures require copying and pasting information between Okta and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

Build an Okta SAML Application

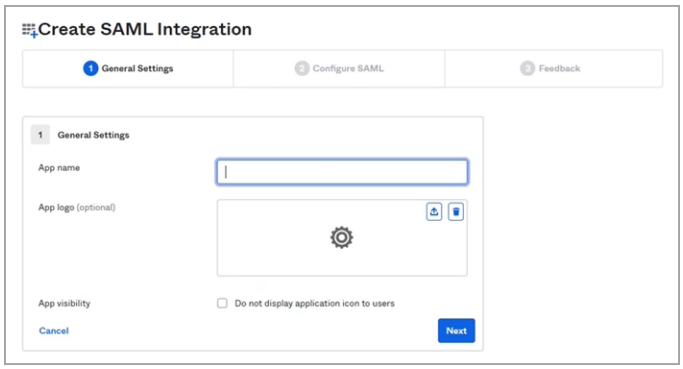
1. From the Okta left navigation menu, click **Applications**.
2. On the Applications page, click **Create App Integration**.



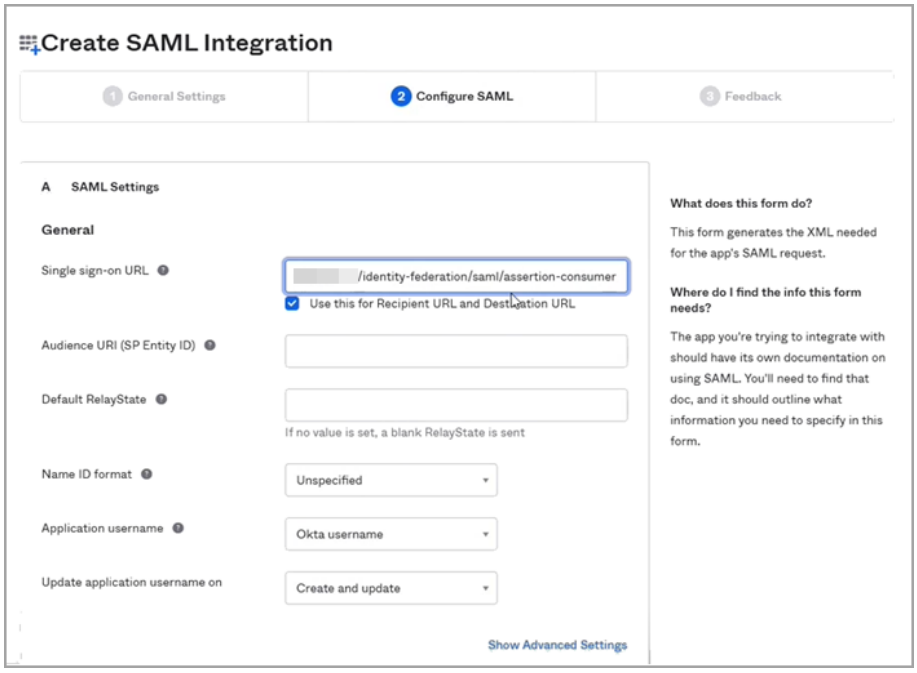
3. On the **Create a new app integration** page, select **SAML 2.0**.



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`.



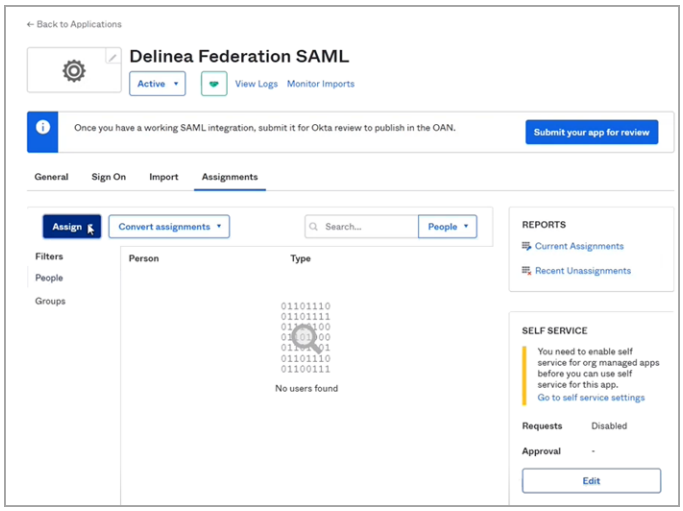
6. Click **Next**.
7. In the SAML Settings section next to **Single sign-on URL**, paste the following:
   `https://[HOST-NAME].delinea.app/identity-federation/saml/assertion-consumer`
8. Replace [HOST-NAME] with the host name you selected when you created your tenant.



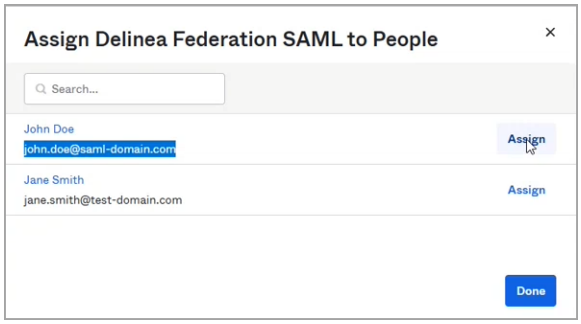
9. Next to **Audience URI (SP Entity ID)**, enter something intuitive, such as `Delinea_Federation`.
10. Scroll down to the **Attribute Statements** section.
11. Add three more blank attribute statements for a total of four.
12. Enter the following into the **Name** and **Value** fields of the four attribute 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.

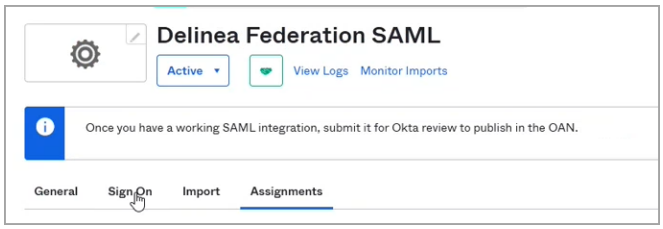


17. Click the **Assign** drop-down and select **Assign to People** or **Assign to Groups**.
18. In the next dialog box, click **Assign** next to the user(s) or group(s) you wish to assign to the federation.

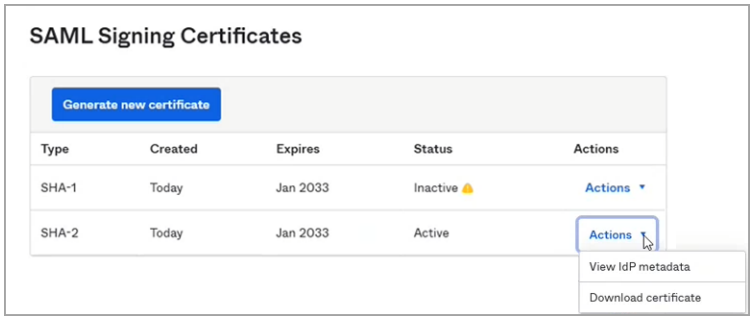


19. Click **Save and Go Back**.

20. Click **Done**.
21. On your Okta new SAML application page, click the **Sign-on** tab.

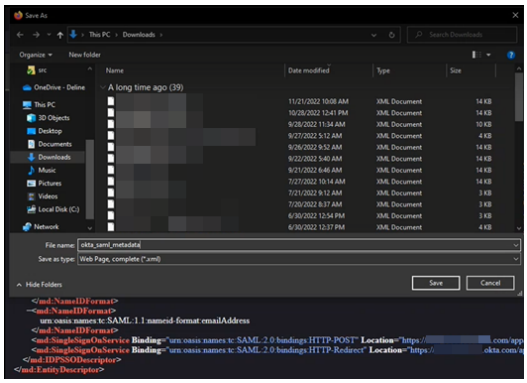


22. Scroll down to **SAML Signing Certificates**.
23. Click the **Actions** drop-down next to the Active certificate and select **Download certificate**.

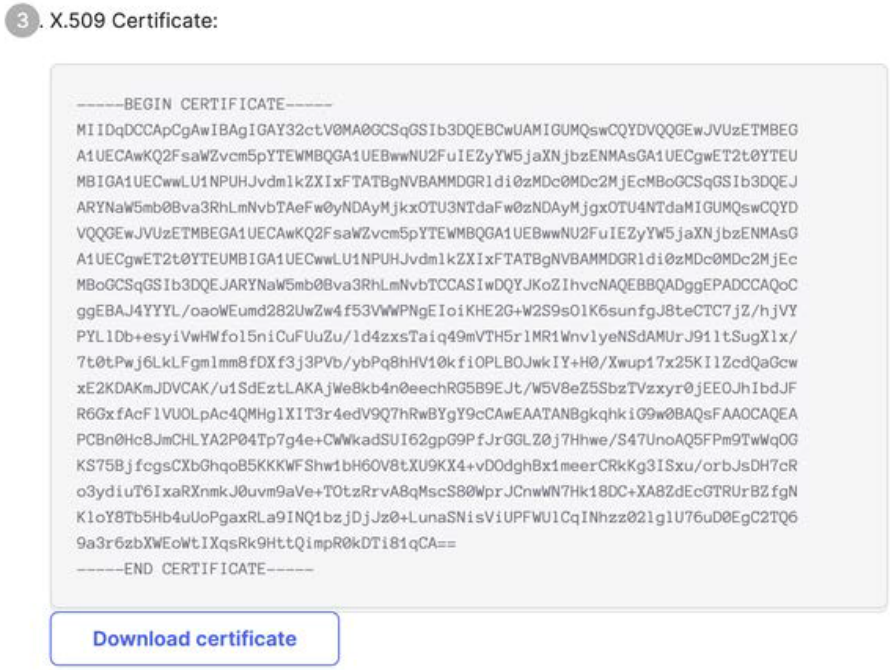


24. Click the **Actions** drop-down next to the Active certificate and select **View IdP metadata**.
25. On the IpD metadata screen, right-click and choose **Save page as...** and select a name to save it as an xml file.

> **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.



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.

Add Provider

Create, review, or manage your SAML provider's configuration. Learn more about Federation Settings

Settings

SAML provider configuration: Select file

Name *: Add name

Protocol: SAML

Status: Enabled

Entity ID *: Add entity URL

IDP certificate: Select file

cer, pem or pkcs7 formats are supported

Signature algorithm	None
Thumbprint	Certificate not provided
Not valid before	Certificate not provided
Not valid after	Certificate not provided
Issuer	None

IDP Login URL *: Add URL

IDP Logout URL: Add URL

Platform callback URL: https://example.delinea.app/identity-federation/saml/assertion-consumer

Platform logout URL: https://example.delinea.app/identity-federation/saml/logout-consumer

Advanced Settings

Customize certificate issuer sent to IDP

Force Authentication (ForceAuthN)

Use Login Hint

Request binding: HTTP-Redirect

Sign Request

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	
EmailAddress	email	Required Attribute
Name	displayname	
[illegible]	sub	Required Attribute
upn	upn	Required Attribute

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
   Copy the Platform Callback URL to paste into the Sign-in redirect URIs field in your new Okta application.
7. **Prompt:** See "Federation Management" on page 52 under Federation Management.
8. **Platform Logout URL**: 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 53 under Federation Management.

Attribute Mappings

See "Attribute Mappings" on page 54 under Federation Management.

Group Mappings

See "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56 under Federation Management.

Domains

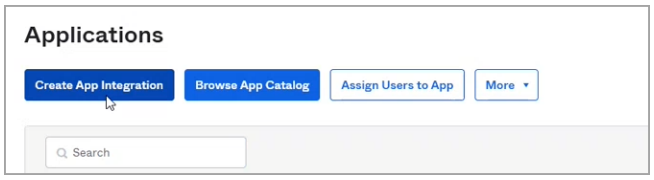
1. Click **Add Domain** and enter the domain from the email addresses of the users you are including in this federation.

When all required fields are populated, click **Add Provider**.

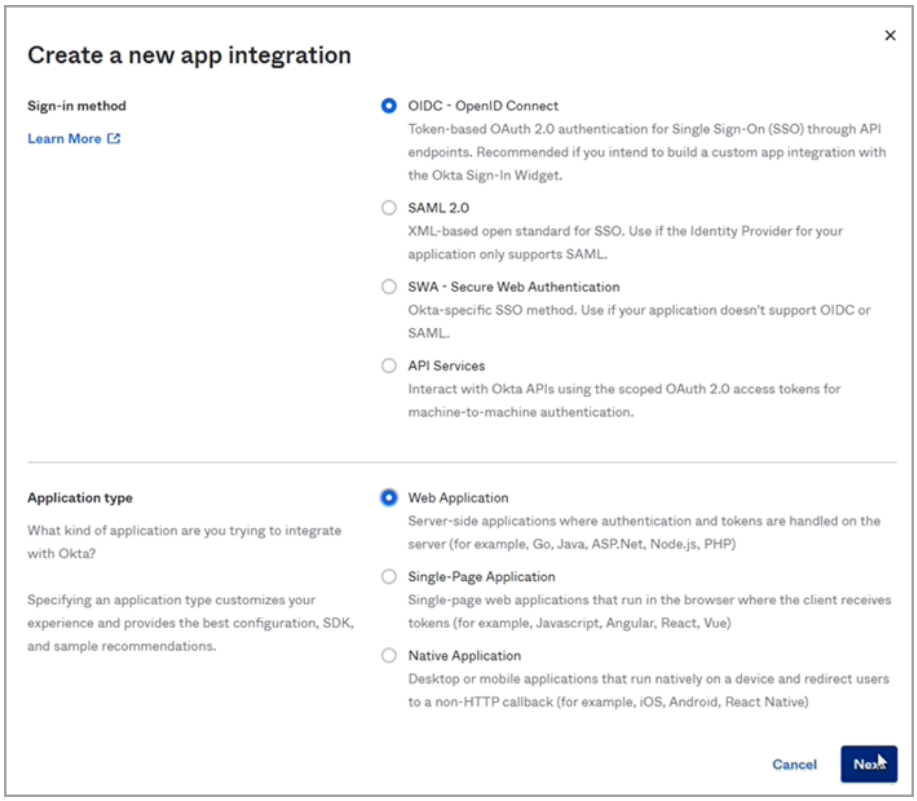
Build an Okta OIDC Application

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.

1. From Okta, click **Applications** from the left navigation menu.
2. 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.

Add Provider

Create, review, or manage your OIDC provider's configuration. Learn more about Federation Settings

Settings

Name *	Add name
Protocol	OIDC
Status	Enabled
Endpoint URL *	Add endpoint URL
Client ID *	Enter client ID
Client secret *	**********
Prompt	Not Specified
Platform callback URL	None

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/nameidentifier	sub	Required Attribute
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	upn	Required Attribute
name	displayname	

Add Attribute Mapping

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME	GROUP

No items found

Add Group Mapping

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	Disabled

Domains

Specify domains users may use as part of their login name

DOMAIN

No items found

Add Domain

4. **Name**: Enter a unique name.
5. **Status**: Select the box next to **Enabled**.
6. **Endpoint URL**: Paste in the Okta domain name copied from your Okta application page. You might need to add https:// to the beginning.
7. **Client ID**: Paste in the Client ID copied from your Okta new OIDC application page.
8. **Client Secret**: Paste in the Client Secret copied from your Okta new OIDC application page.
9. **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.

Note: If you need an updated Platform Callback URL, finish the steps below until you click **Add Provider**. An updated Platform Callback URL with then be available for copying from the interface.

Attribute Mappings

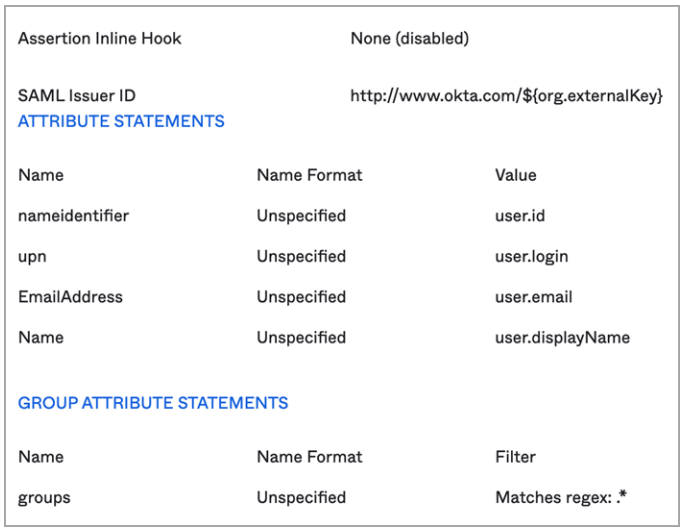
In the upn field, change the text to **preferred_username**.

See "Attribute Mappings" on page 54 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**.
11. Click the **General** tab.
12. Edit the SAML integration and click **Next** to configure the SAML settings.
13. 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: .*

14. Set the following:
    a. **Name**: `groups`
    b. **Name format**: `Unspecified`
    c. **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.
15. Click **Next** and **Save**.

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 "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56 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**.

Integrating OneLogin

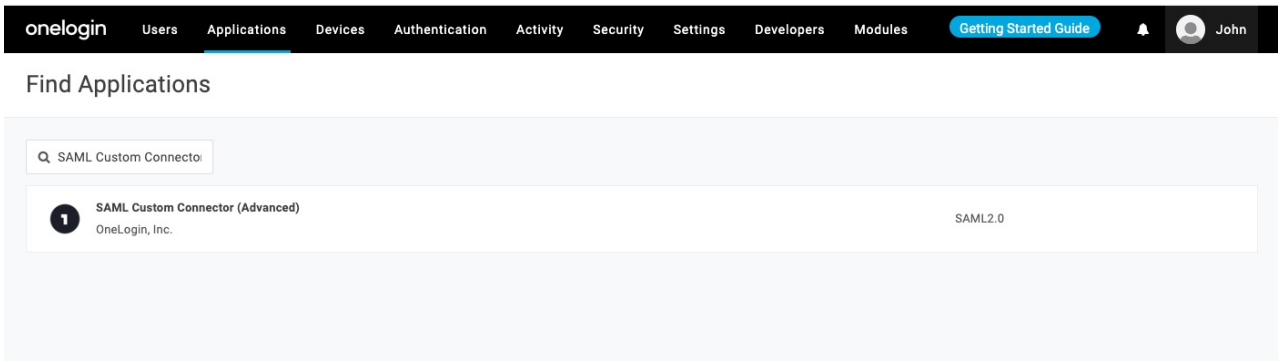
On the Delinea Platform, you need admin with federation privileges.

In OneLogin, you need admin access to create a SAML and OIDC applications.

The following procedures require copying and pasting information between Onelogin and the Delinea Platform. We recommend opening both applications in separate browser windows.

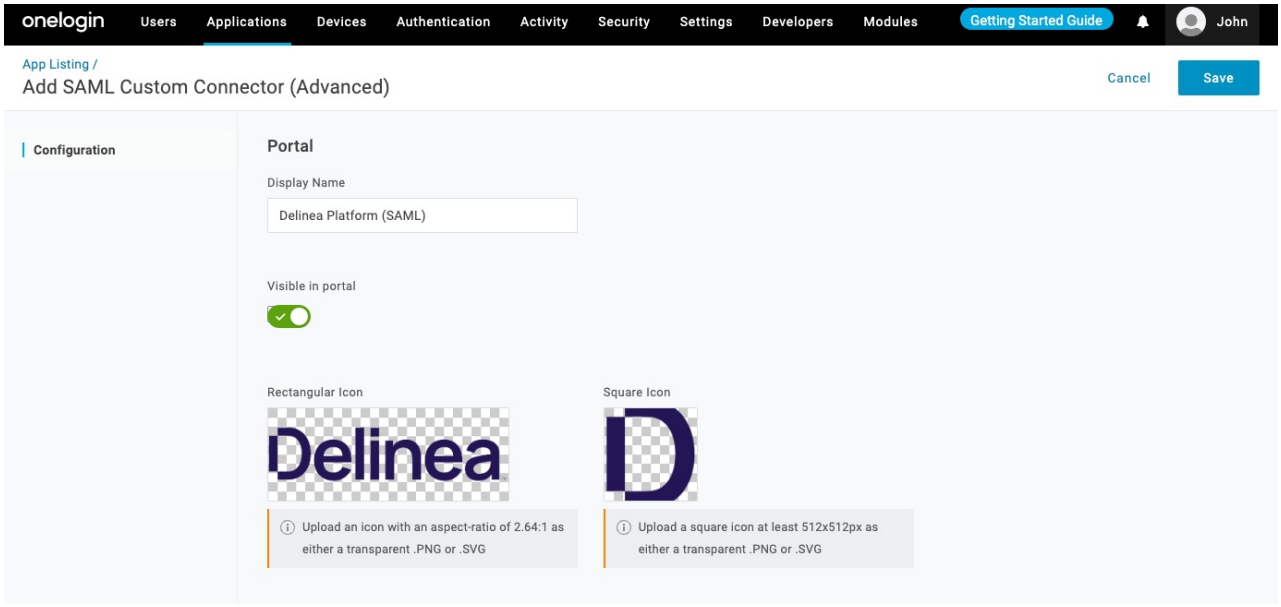
Build a OneLogin SAML Application

1. Log in to the OneLogin Dashboard.
2. Navigate to **Applications** > **Add App**.
3. Search for SAML, and select **SAML Custom Connector (Advanced)**.

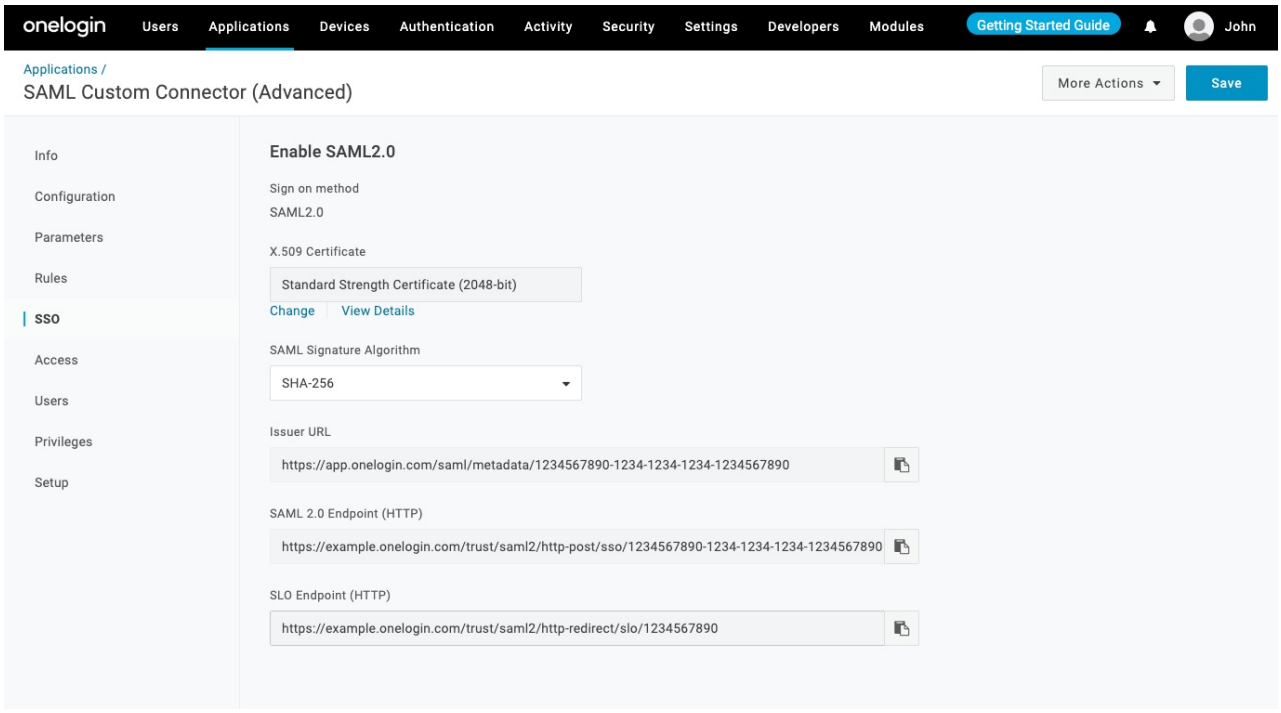


4. When prompted, update the **Display Name** of your application.
   - Optionally, change **Visible in portal** setting
   - Optionally, provide images for the application, and a description

5. Click **Save**.

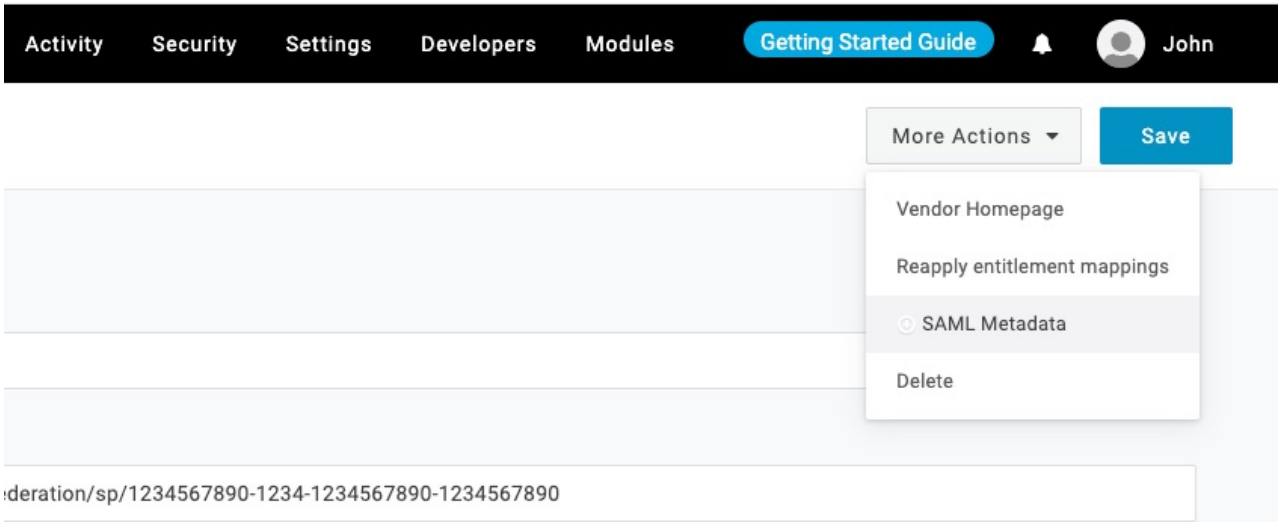


6. From the left navigation, select the **SSO**.
7. Update the **SAML Signature Algorithm** to **SHA-256**.
8. Click **Save**.



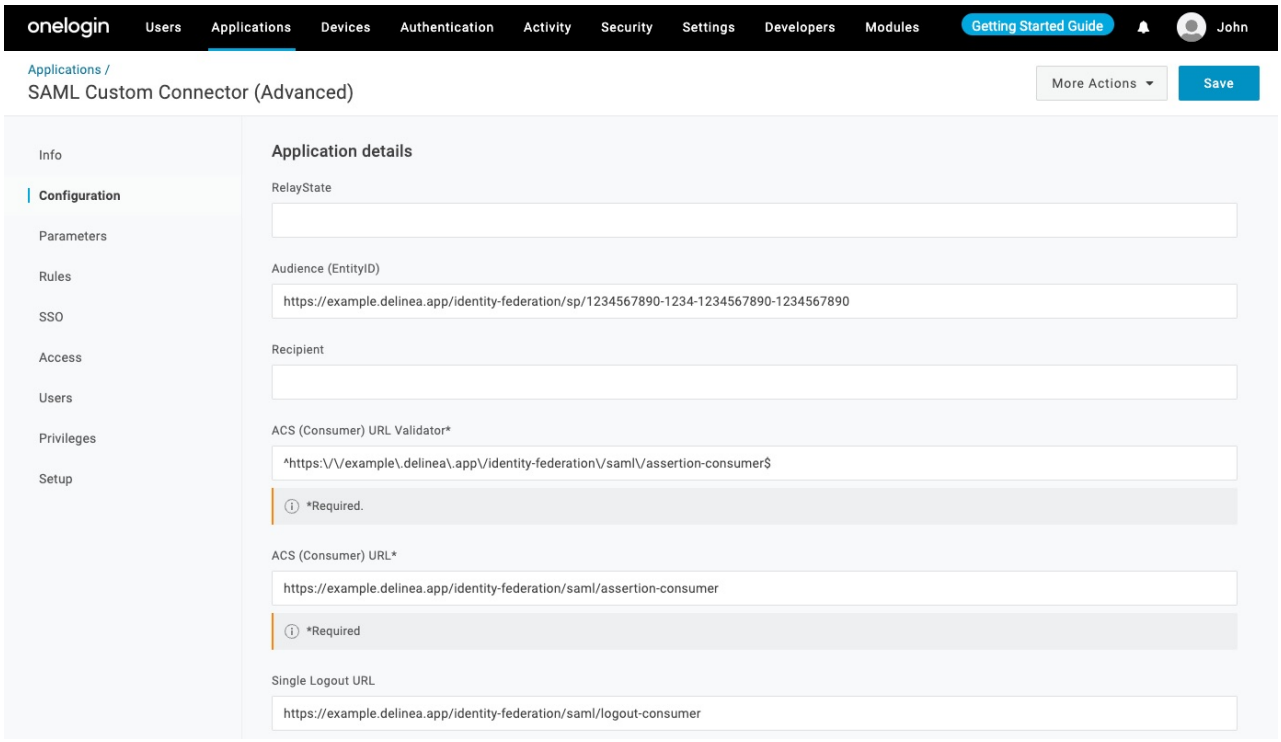
9. Navigate to **More Actions** from the top right menu.

10. Download **SAML Metadata**.



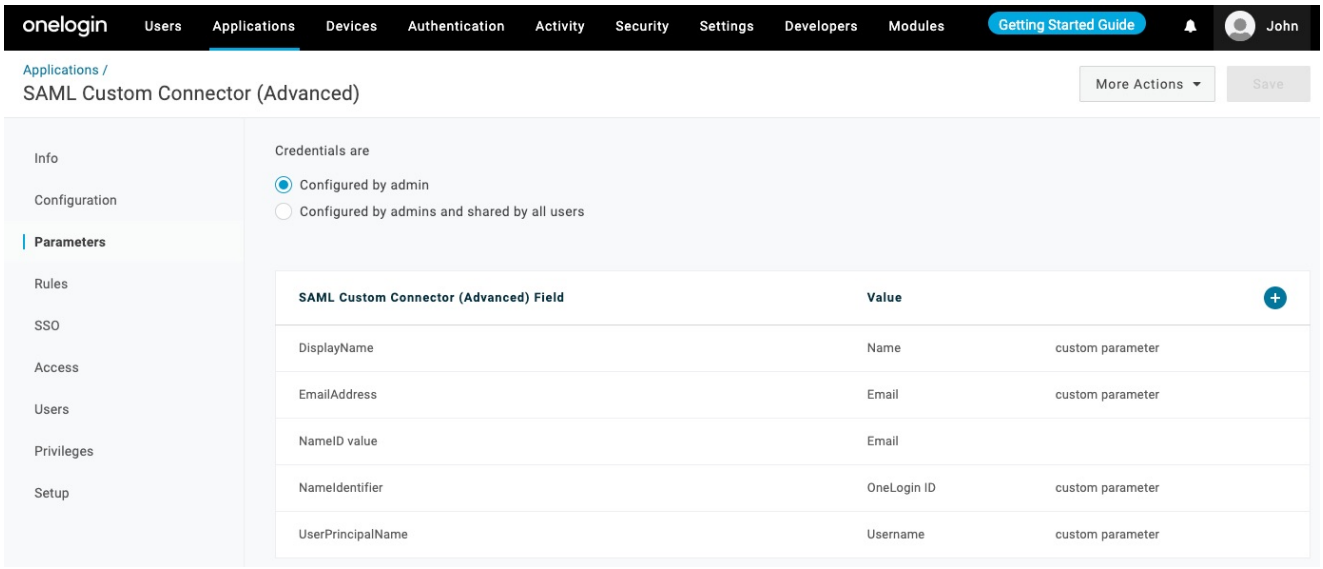
11. Navigate to **Configuration** and fill out the below information.

OneLogin setting	Delinea Platform setting
Audience (Entity ID)	From **Advanced Settings** select and use the **Customize certificate issuer sent to IDP** value. Note: Currently, this value is not available until the federation provider is created in the Delinea platform.
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



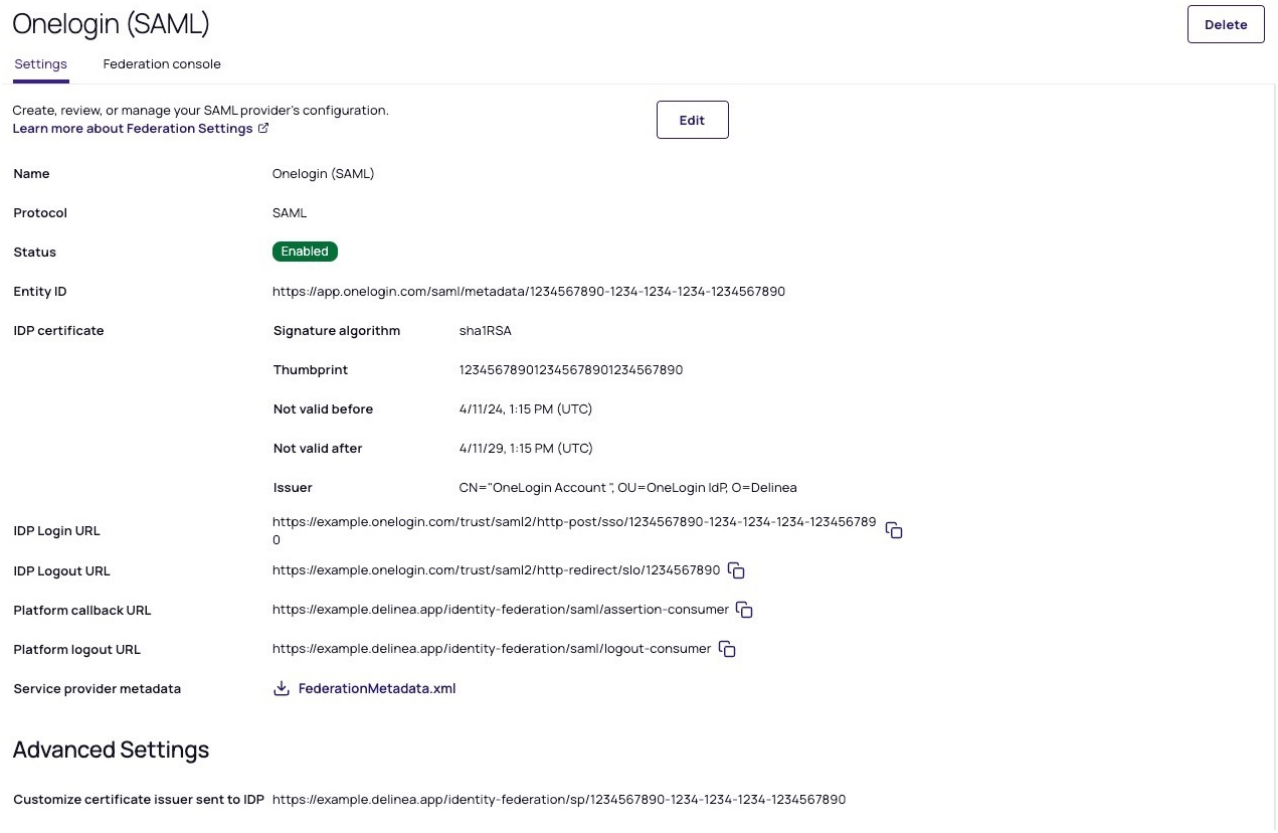
12. Click **Save**.
13. Go to **Parameters** and add the following custom attributes. For each field, make sure the **Include in SAML assertion** flag is selected.

SAML Custom Connector (Advanced) Field	Value
DisplayName	Name
EmailAddress	Email
NameIdentifier	OneLogin ID
UserPrincipalName	Username



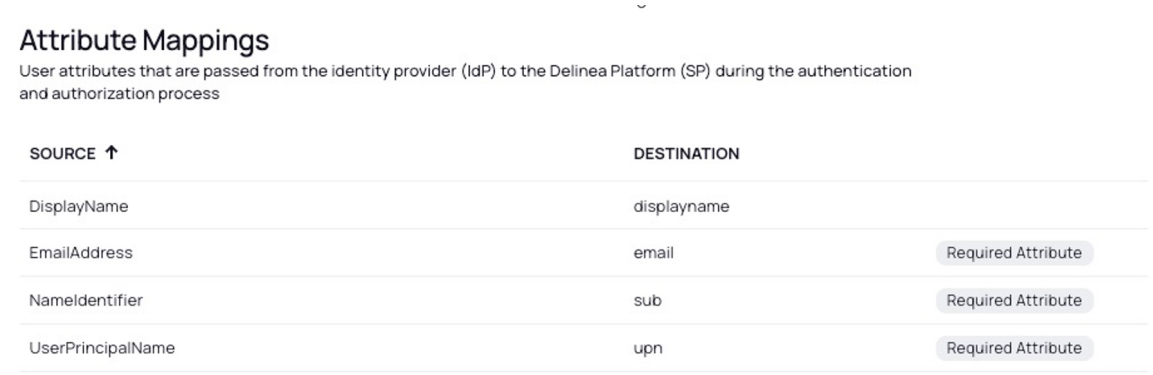
Add a Delinea Platform SAML Provider

1. Log in to the Delinea Platform.
2. Navigate to **Settings** > **Federation providers**.
3. Click **Add Provider** and select **SAML**.
4. In the SAML provider configuration click **Select file** and upload the SAML metadata file previously downloaded from Onelogin.
5. Click the **Apply** button. This step will also save the provider.
6. Click **Edit** to continue updating the SAML provider.
7. In the **Name** field, set the unique name for the provider.
   - Optionally, set the **Status** to Enabled.
8. In the Advanced Settings, enable **Customize certificate issuer sent to IDP**.



9. In the Attribute Mappings section, update these attributes as follows:

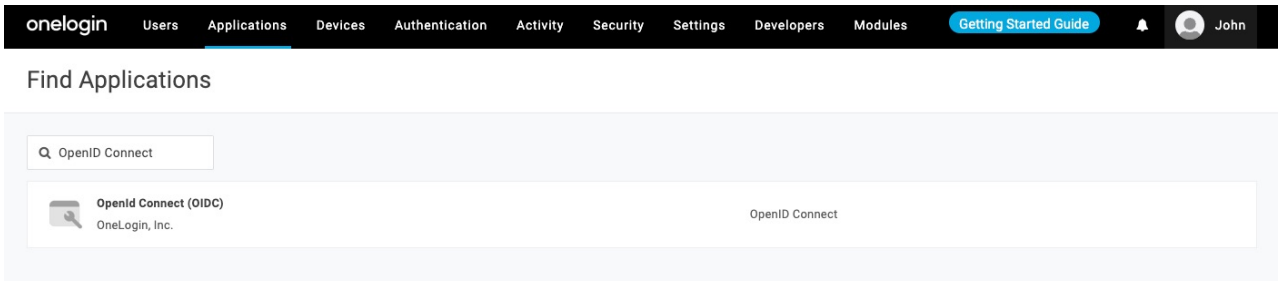
Source	Destination
DisplayName	displayname
EmailAddress	email
NameIdentifier	sub
UserPrincipalName	upn



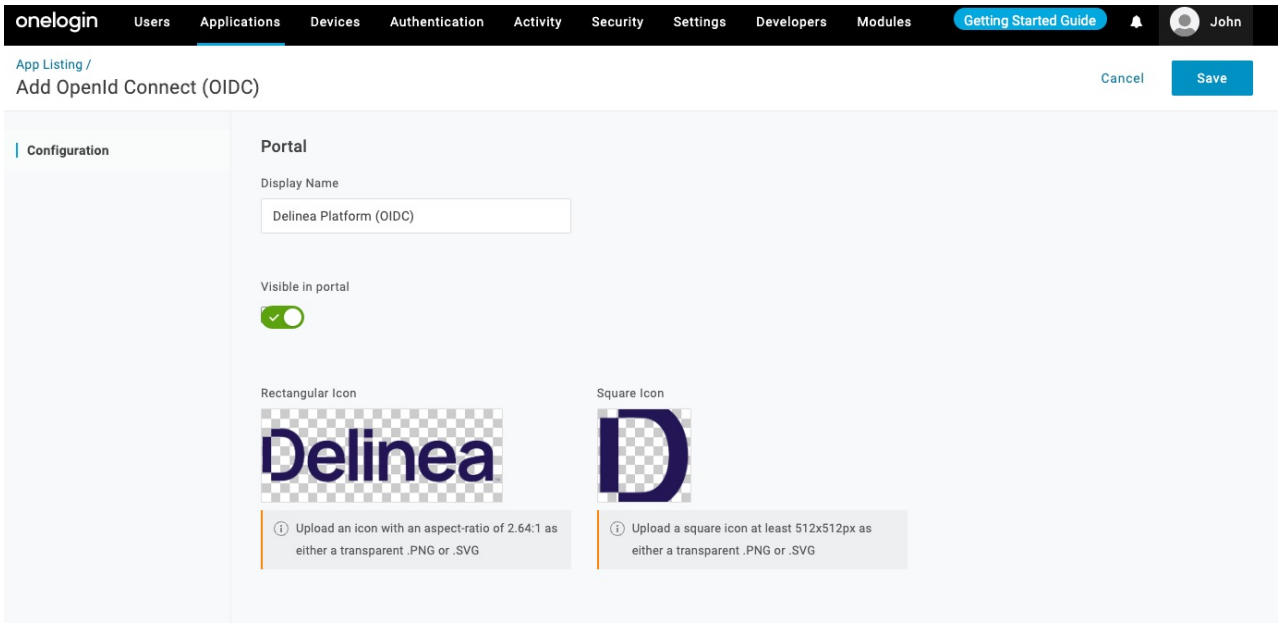
10. In the Domains section click **Add Domain** and add your domain(s).
11. Click **Save**.

Build a Onelogin OIDC Application

1. Log in to the OneLogin Dashboard.
2. Navigate to **Applications** > **Add App**.
3. Search for **OpenID Connect (OIDC)**.

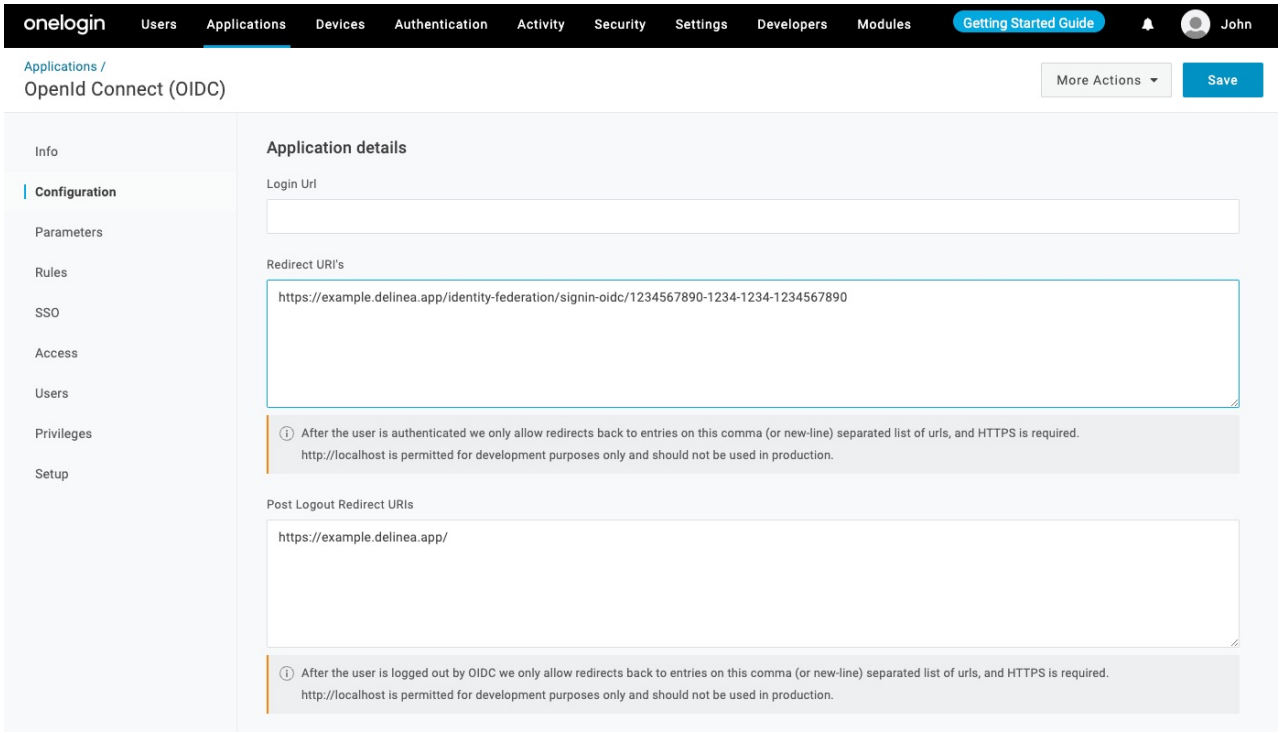


4. When prompted, update the **Display Name** of your application.
5. Optionally, provide images for the application, and a description.
6. Click **Save**.

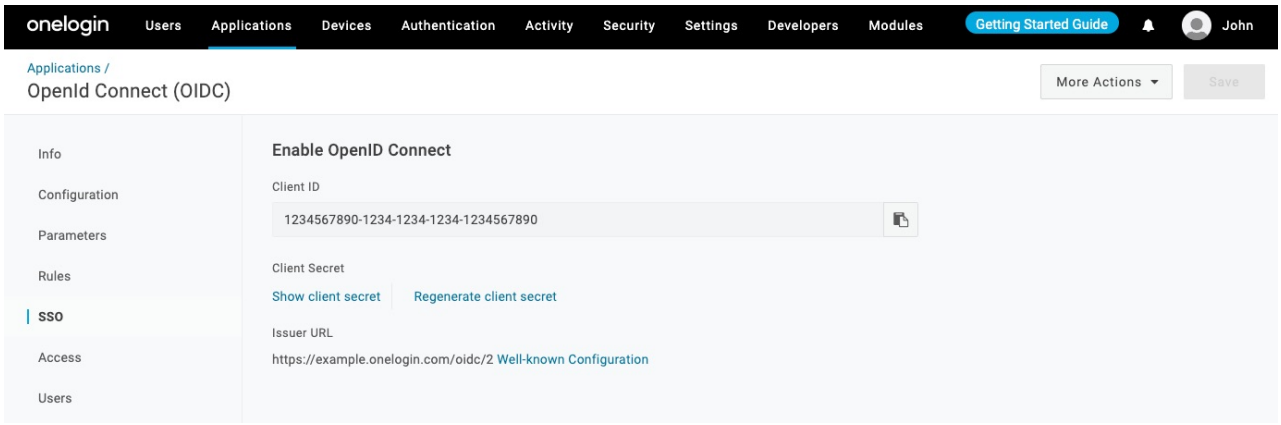


7. Continue with Configuration of the newly created application by updating the Redirect URI.

OneLogin	Delinea Platform
Login URL	Optional. You can set this to your tenant URL (e.g. https://example.delinea.app)
Redirect URL	Platform Callback URL This value cannot be blank. http://localhost may be used until the value is created in the Delinea platform.

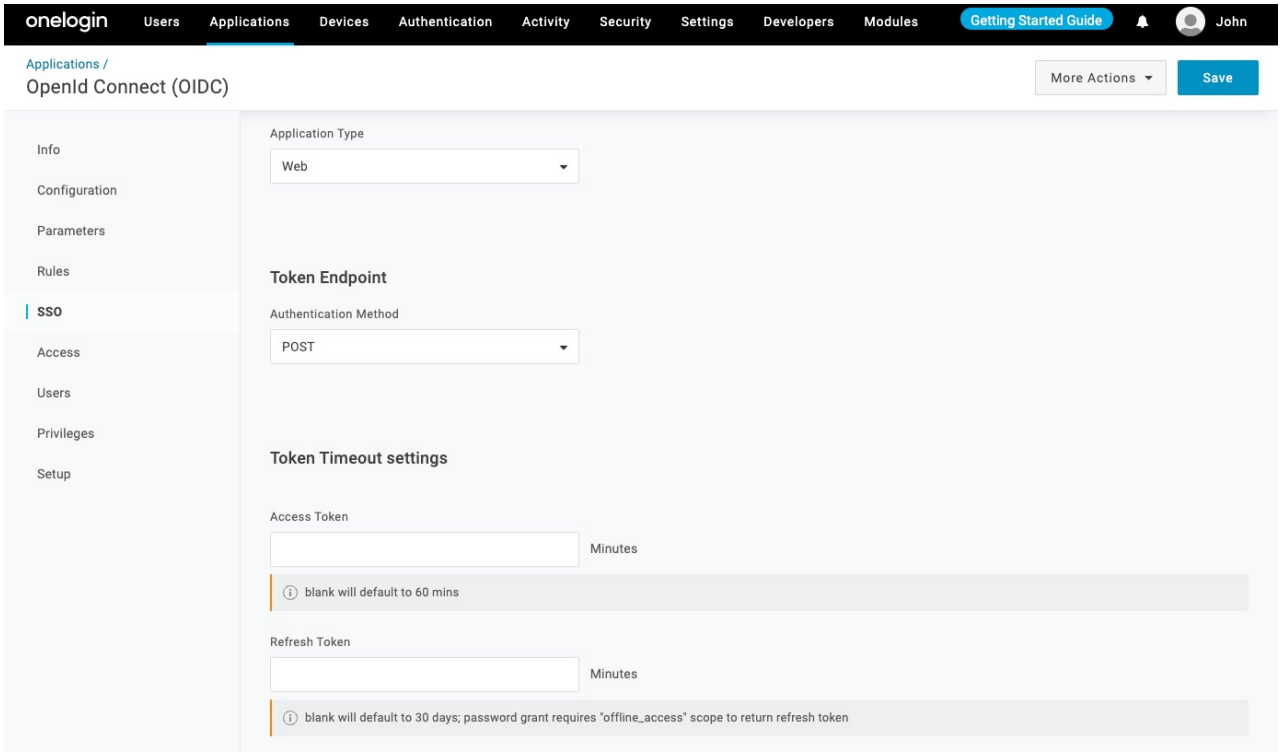


8. Next, navigate to **SSO**, and make note of the **Client ID**, **Client Secret**, and **Issuer URL** for use with your OIDC-enabled application. You would need this information when setting up Onelogin federation provider in Delinea Platform



9. Continue with the SSO settings.

Setting	Value
Application Type	Web
Token Endpoint	POST



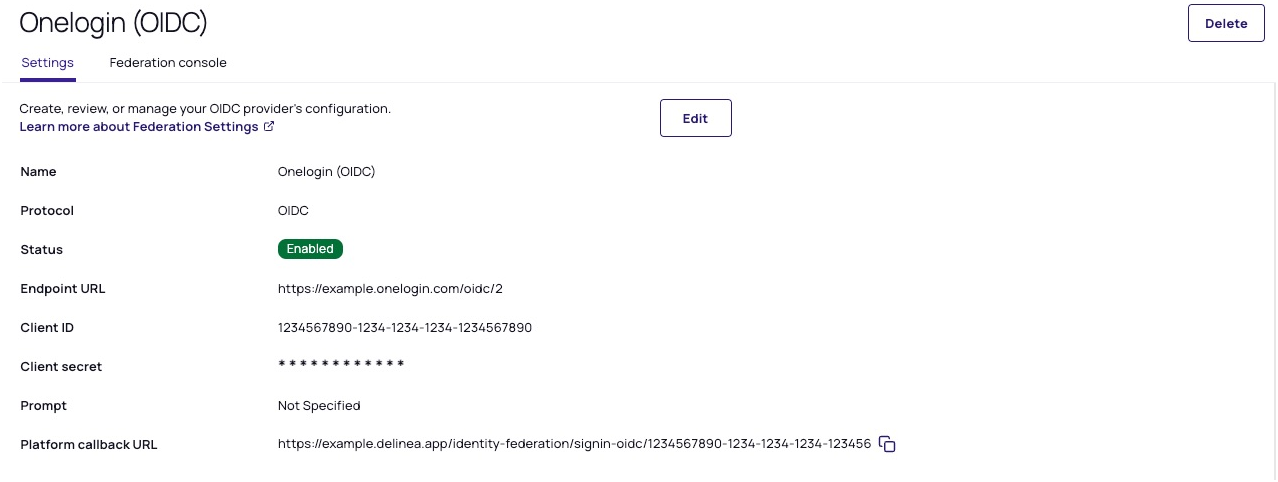
10. Save the application settings.
11. Optionally, on the Users page, add users/groups who should have access to this application.

Add a Delinea Platform OIDC Provider

1. Navigate to **Settings** > **Federation Providers**.
2. Create a new OIDC provider.
3. Provide a unique name for your provider (e.g. Onelogin - OIDC).
4. Update these settings:

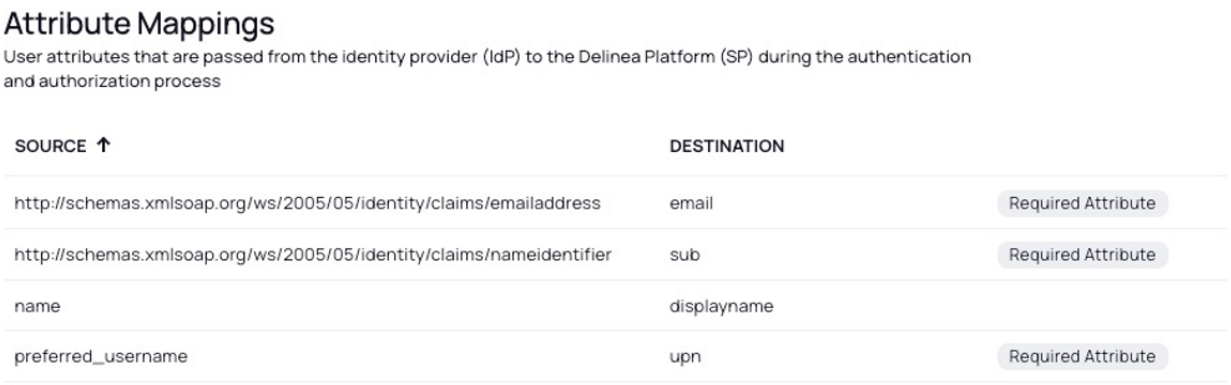
Delinea Platform	OneLogin
Endpoint URL	Issuer URL

Delinea Platform	OneLogin
Client ID	Client ID
Client Secret	Client Secret



5. Click **Add Provider**.
6. Make note of the **Platform Callback URL** as this is needed in your OneLogin application and update the Redirect URIs in the OneLogin application.
7. Click **Edit** and Update these 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



8. Add your domain(s).
9. Optionally enable the **Status** of the provider.
10. Click **Save** to save your updated settings.

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 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 Ping Identity (PingOne), leveraging SAML 2.0 or OIDC.

Note: The following procedures require copying and pasting information between Ping Identity and the Delinea Platform. We recommend opening both applications before you begin, and keeping both open until you are finished.

Note: To synchronize newly-federated users and groups, see Federation Management.

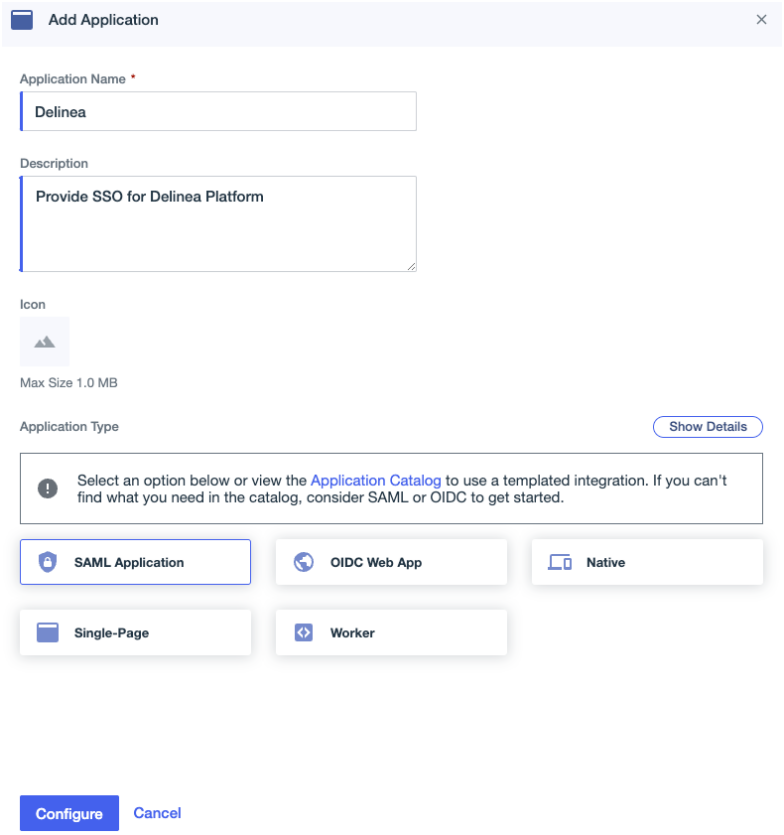
Prerequisites

- In Ping Identity (PingOne), ensure that you have administrative privileges to manage application settings.
- On the Delinea Platform, ensure that you have administrative privileges to manage federation provider settings.

Note: We recommend having Ping Identity and the platform UI open in separate tabs in your web browser to switch between them easily.

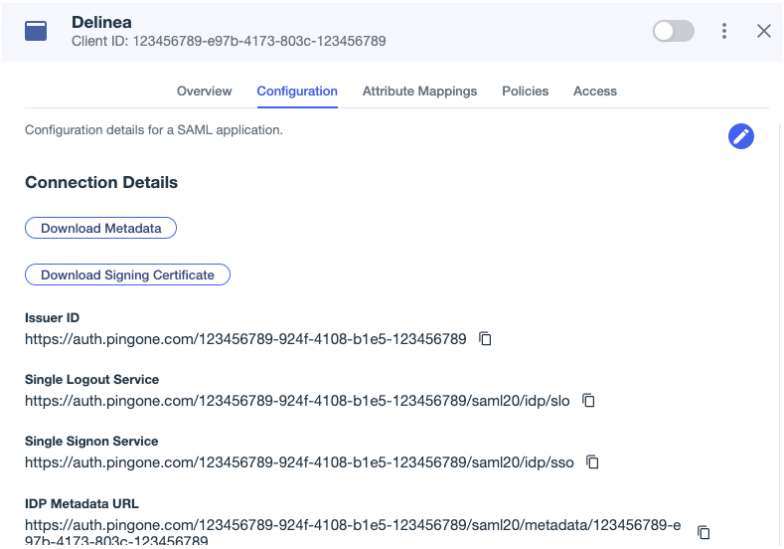
Build a Ping Identity SAML Application

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**.



5. Click **Configure**.
6. In the SAML Configuration section, choose **Manually Enter**.
   a. **ACS URL**: `https://<tenant-name>.delinea.app/identity-federation/saml/assertion-consumer`
   b. **Entity ID**: Set it to `none`. We will revise this setting in the forthcoming instructions.

7. Clicking **Configuration** > **Connection Details**
8. 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.

Add Provider

Create, review, or manage your SAML provider's configuration. Learn more about Federation Settings

Settings

SAML provider configuration: Select file

Name *: Add name

Protocol: SAML

Status: Enabled

Entity ID *: Add entity URL

IDP certificate: Select file

cer, pem or pkcs7 formats are supported

Signature algorithm	None
Thumbprint	Certificate not provided
Not valid before	Certificate not provided
Not valid after	Certificate not provided
Issuer	None

IDP Login URL *: Add URL

IDP Logout URL: Add URL

Platform callback URL: https://example.delinea.app/identity-federation/saml/assertion-consumer

Platform logout URL: https://example.delinea.app/identity-federation/saml/logout-consumer

Advanced Settings

Customize certificate issuer sent to IDP

Force Authentication (ForceAuthN)

Use Login Hint

Request binding: HTTP-Redirect

Sign Request

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	
EmailAddress	email	Required Attribute
Name	displayname	
[illegible]	sub	Required Attribute
upn	upn	Required Attribute

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:
     - 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
    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
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 53 under Federation Management.

Attribute Mappings

Source | Destination

- EmailAddress | email*
- DisplayName | displayname
- saml_subject | sub*
- upn | upn*

Also see "Attribute Mappings" on page 54 under Federation Management.

Group Mappings

See "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56 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

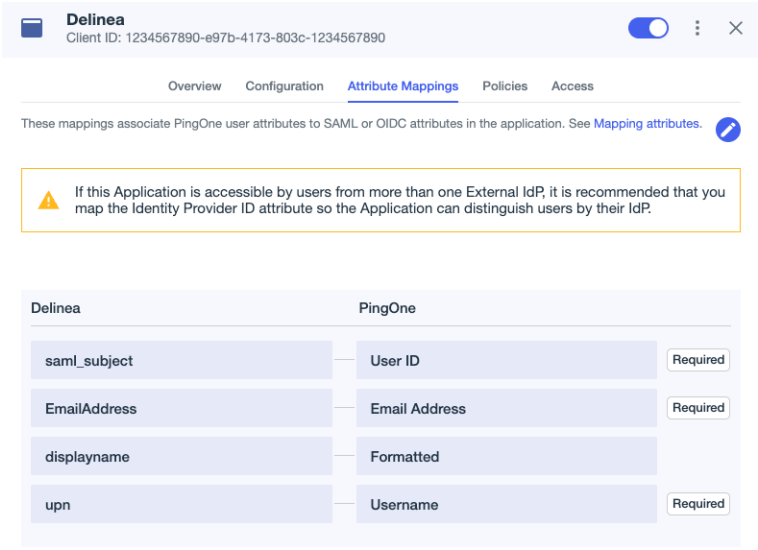
Update Entity ID

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)

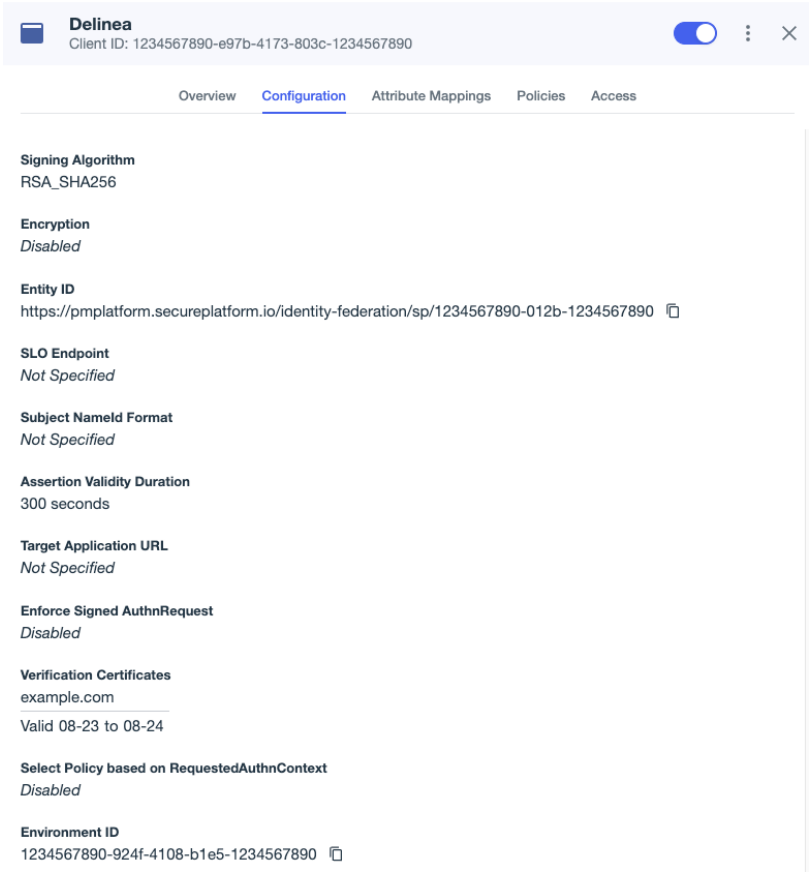
- upn | Username (mark as required)



3. Click **Save**.

Activate the Application

Activate the application by engaging the toggle button in the top-right corner.

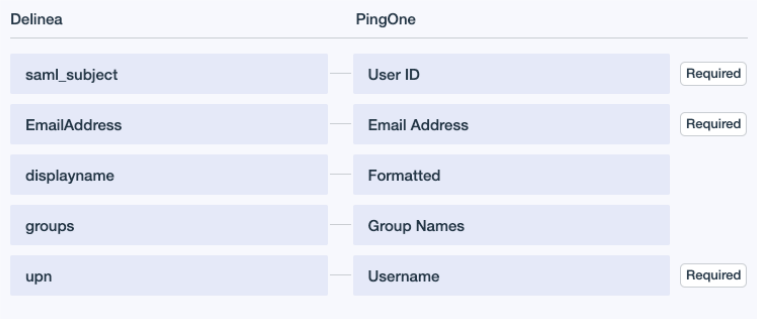


Map Ping Identity and Platform Groups

From Your Ping Identity Application

Users can be automatically assigned to groups on the platform by sending their group memberships from PingOne.

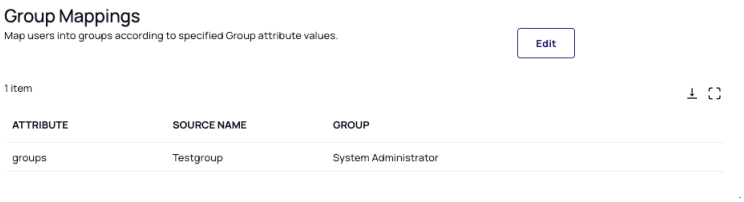
1. Go to the PingOne application > **Attribute Mappings**.
2. Click **Edit**.
3. Add a new attribute by clicking the **+ Add** button.
   The new attribute should be as follows:
   groups | Group Names



4. Click **Save**.

From the Platform

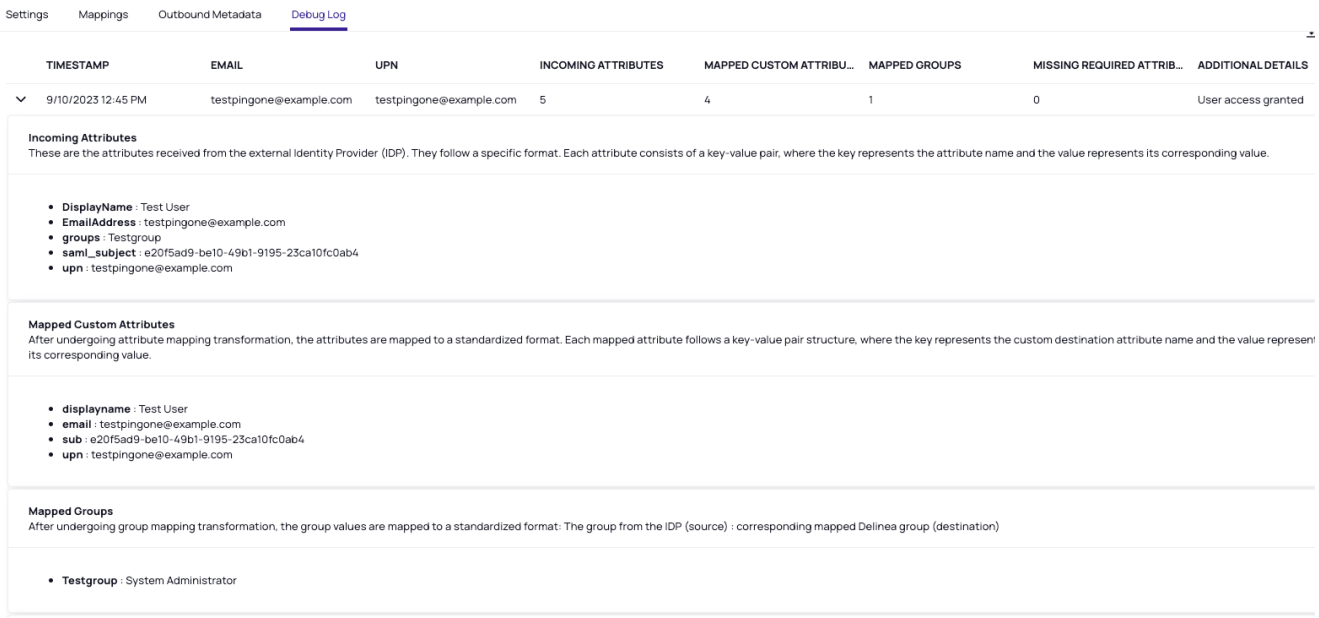
1. Click **Settings** from the left navigation, then select **Federation Providers**.
2. Click the Ping One provider.
3. Click **Edit**.
4. Click **Add Group Mapping**.
   - **Attribute**: groups
   - **Source Name**: Use the PingOne group.
   - **Group**: Select the Delinea group.



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.

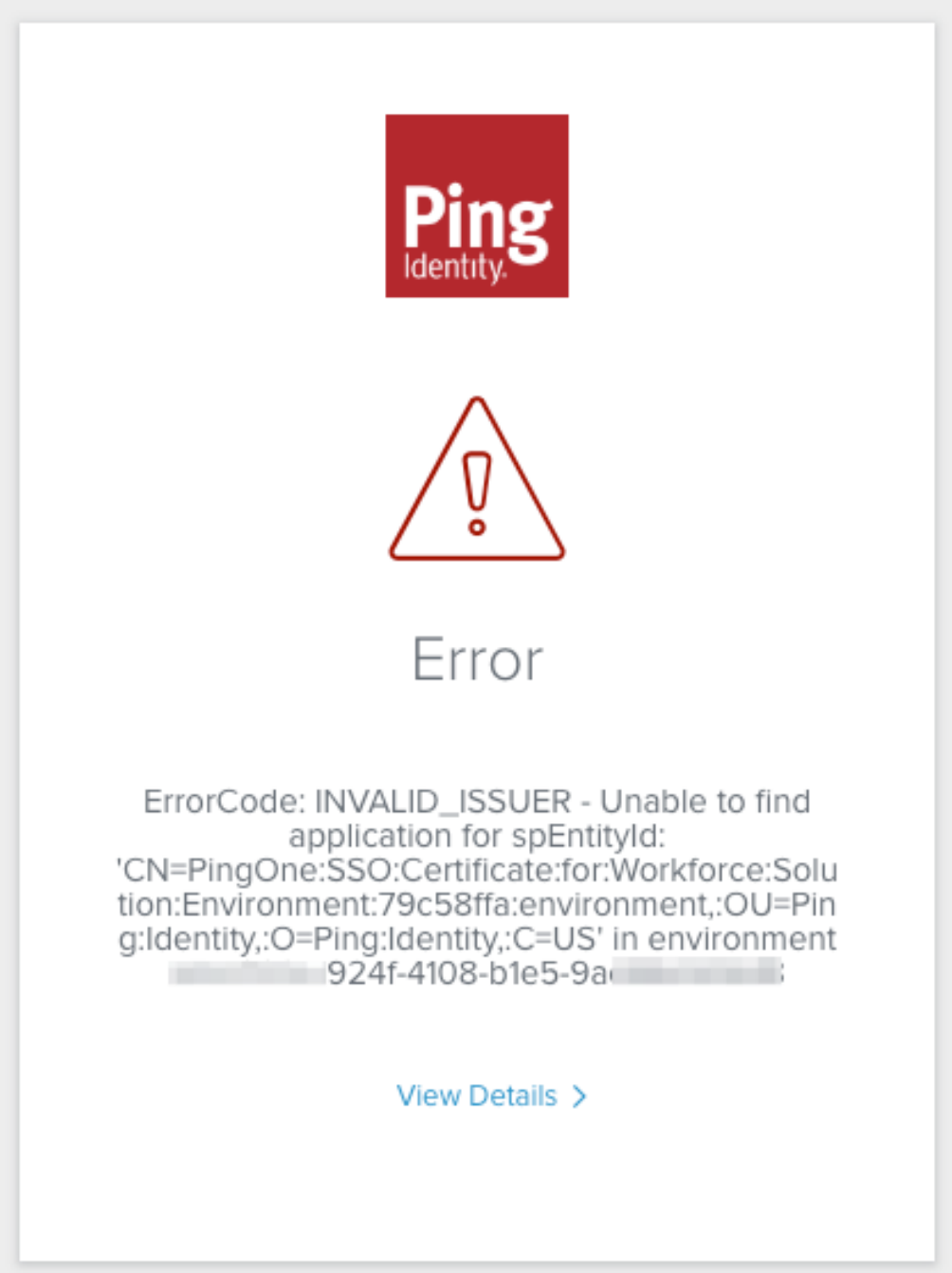
Note: For additional details regarding troubleshooting federated logins, refer to *Debugging the Federation Log* on the "Federation Management" on page 52 page.



Troubleshooting

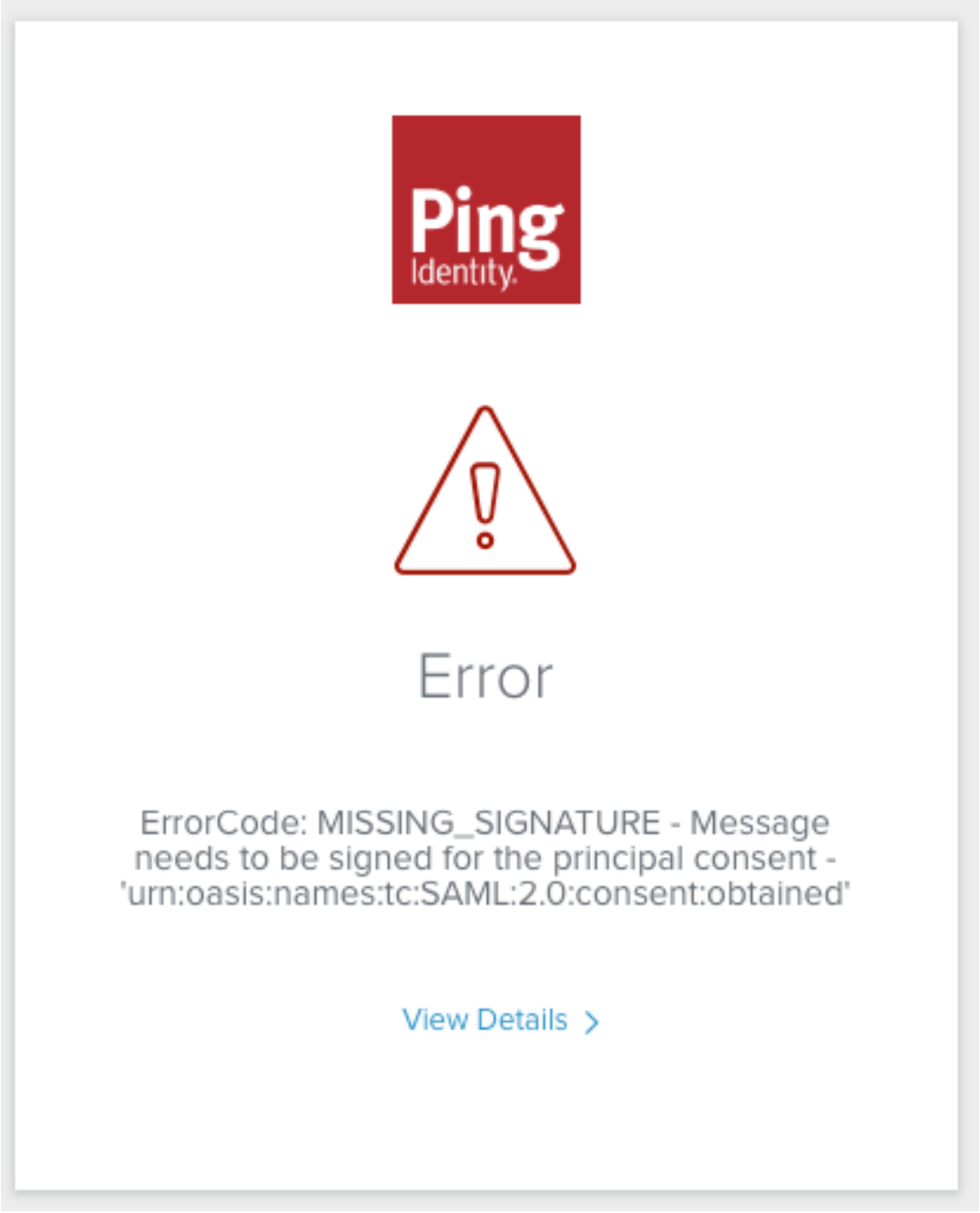
ErrorCode: Invalid Issuer - Unable to find application for spEntityId

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.



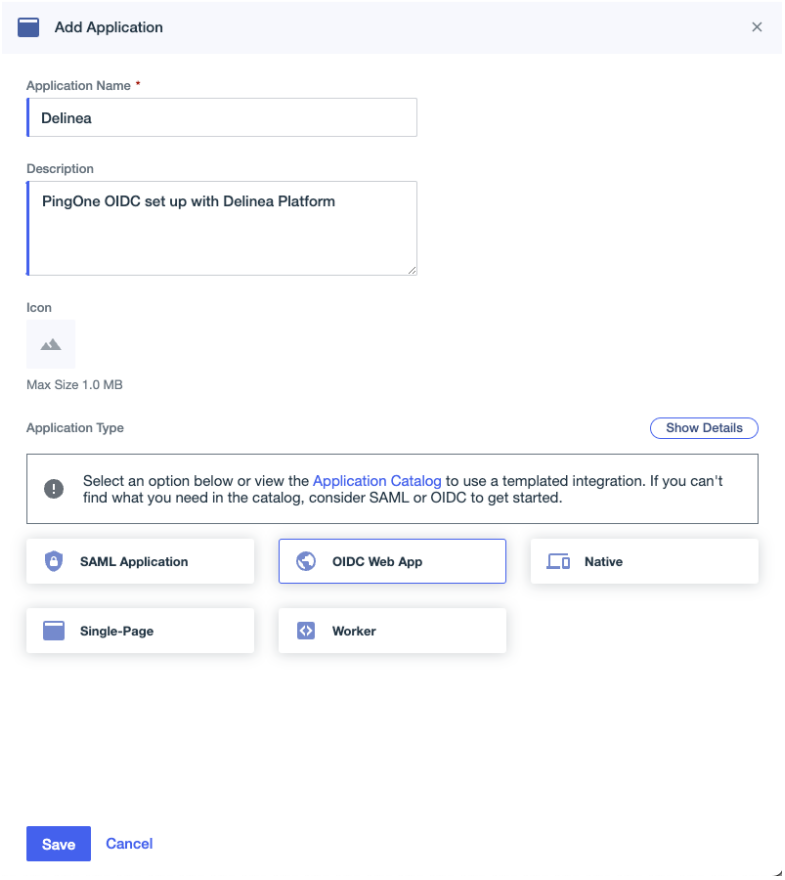
ErrorCode: MISSING_SIGNATURE – Message needs to be signed for the principal consent

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**.



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.

Add Provider

Create, review, or manage your OIDC provider's configuration. Learn more about Federation Settings

Settings

Name *	Add name
Protocol	OIDC
Status	Enabled
Endpoint URL *	Add endpoint URL
Client ID *	Enter client ID
Client secret *	**********
Prompt	Not Specified
Platform callback URL	None

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/nameidentifier	sub	Required Attribute
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	upn	Required Attribute
name	displayname	

Add Attribute Mapping

Group Mappings

Map users into groups according to specified group attribute values.

ATTRIBUTE	SOURCE NAME	GROUP

No items found

Add Group Mapping

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	Disabled

Domains

Specify domains users may use as part of their login name

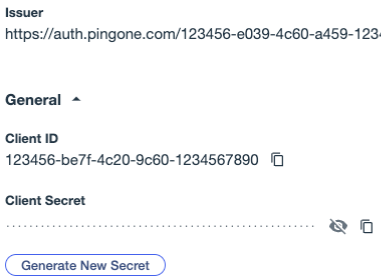
DOMAIN

No items found

Add Domain

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 "Federation Management" on page 52 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 139 on this page.

Also see "Group Mappings" on page 55 under Federation Management.

User Mappings

See "User Mappings" on page 56 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

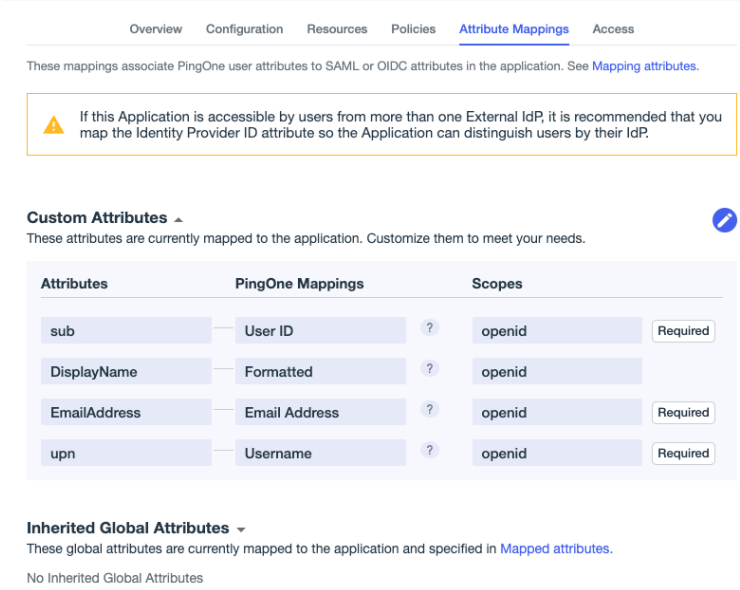
Signoff URLs
None Specified

Token Auth Method
Client Secret Post

Require Pushed Authorization Request
Not Selected

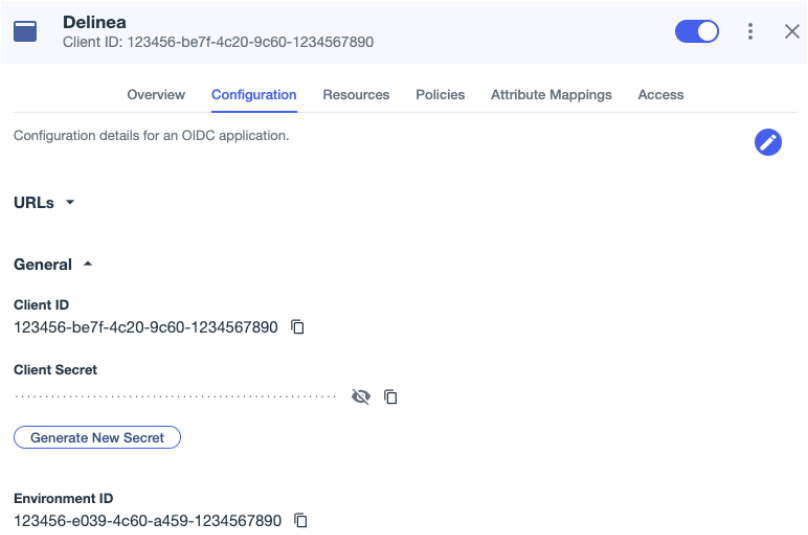
Attribute Mappings

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)



Enabling the Application

Activate the application by enabling the toggle button in the top-right corner.



Test Connection

Follow the steps under "Test Connection" on page 140 in the SAML portion of this document.

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.

About MFA

MFA uses two or more of the following factors to authenticate users logging into a system:

- Something you *know* (such as a password or your birth year)
- Something you *have* (a hardware authenticator such as a smart phone, RSA security token , or a Fido or PIV YubiKey)
- Something you *are* (biometric factors such as fingerprints or retina scans)

Although single-factor Authentication (SFA) was once the standard authentication method, it is grossly inadequate today. SFA requires users to satisfy just one factor to log in, almost always a password. A user typically creates a password that is easy for them to remember, using combinations of birthdays, pet names, and other personal information. But a cyber criminal can easily discover this information using Internet searches, then generate many potential password matches using bots that combine letters, numbers, and other characters.

Platform MFA has two components: Identity MFA profiles and Identity Policies.

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

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.
- Identity MFA. 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 into the Delinea Platform.
- RADIUS Configuration. You can use your RADIUS server to authenticate users 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.

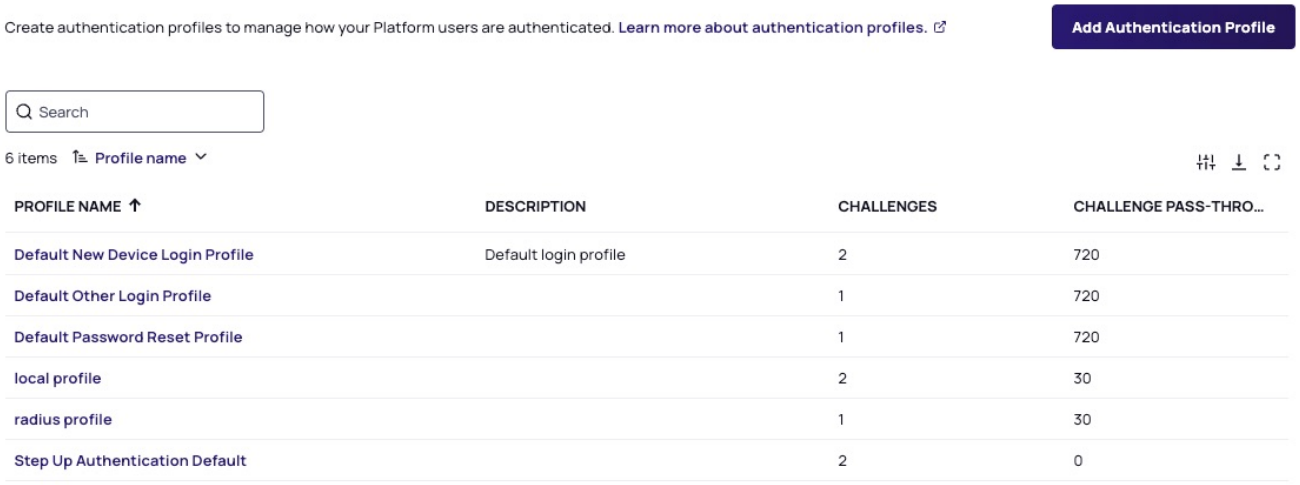
Identity MFA Profiles

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.

Authentication profiles work with identity policies (see Identity Policies), which determine whether and when a user is presented with the challenges specified in the associated authentication profile.

View Authentication Profiles

Click **Settings** from the left navigation, then click **Authentication profiles**.



Platform comes with four built-in authentication profiles:

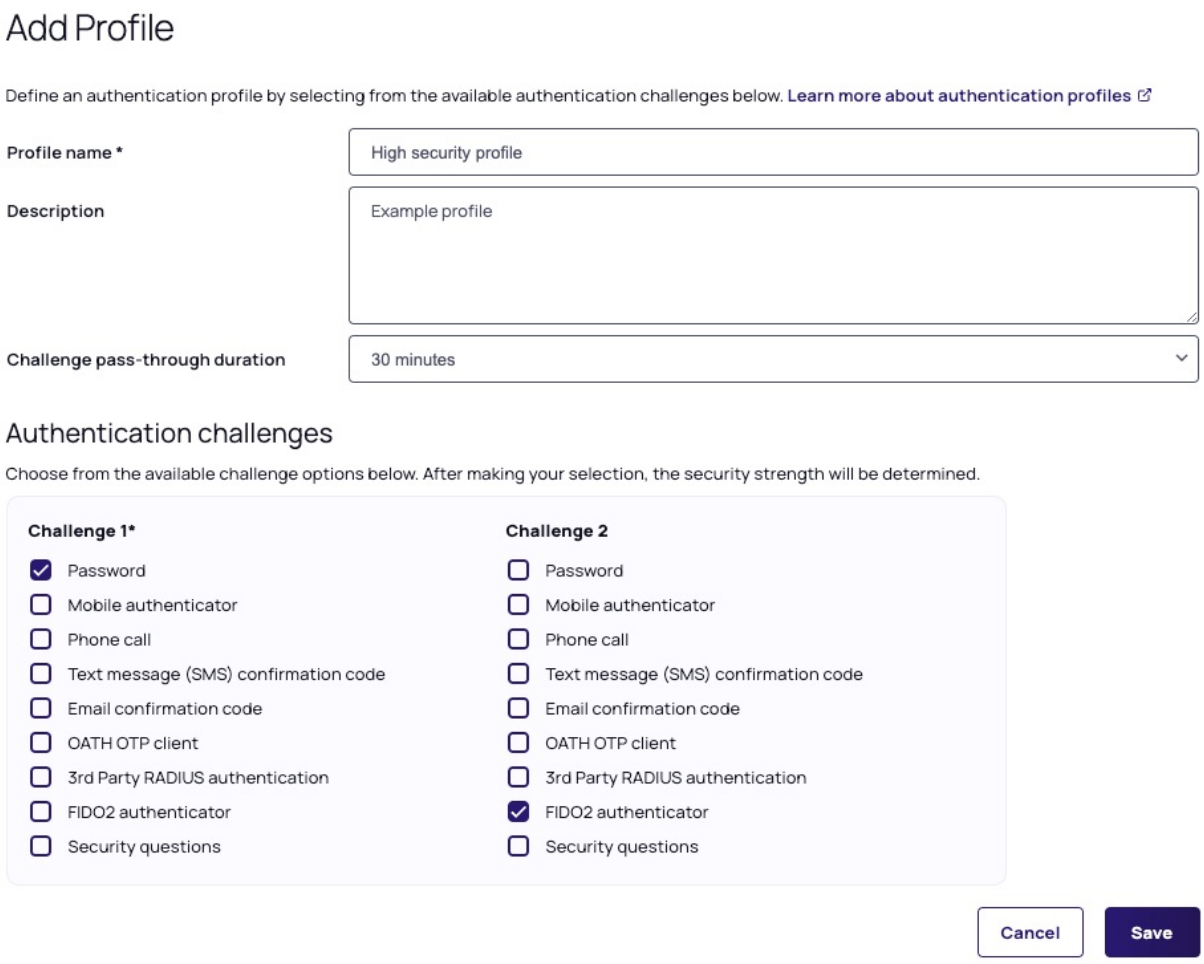
- **Default New Device Login Profile**: Uses Password for the first challenge. For the second challenge, it gives the user options to use Mobile Authenticator, Text message (SMS) confirmation code, Email confirmation code, or OATH OTP Client. 12-hour pass-through duration.
- **Default Other Login Profile**: 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. Populate the fields on the form:

- **Profile name**: a unique name for the profile
- **Description**: a brief description of the profile
- **Challenge pass-through duration**: Choose an option from the drop-down menu to set the time that must elapse before a user is re-prompted for MFA authentication. The default is 30 minutes.
- **Authentication challenges**: Select one or more of the authentication mechanisms available for Challenge 1 and Challenge 2.



3. When you are finished, 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 the user fails the first challenge and the second challenge is SMS, email, or phone call, the default configuration is that Platform will not send the SMS/email or trigger the phone call.

Authentication Challenges

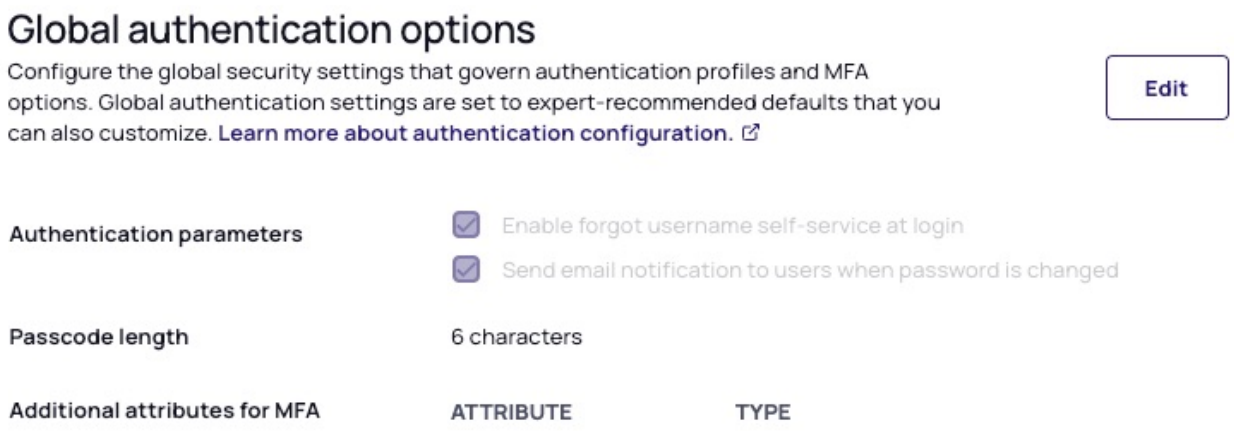
You can select the authentication challenges available to users. However, the challenges actually presented to the user depend on the account's properties. For example, if you select all the mechanisms but a user account has only a username and email address, then the login prompt will present only those two challenges.

The following mechanisms are available:

- **Password**: The user is prompted for either their Active Directory password or Platform account password.
- **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 into the login prompt.
- **Phone Call**: 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**: 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**: Platform sends an email to the user with a one-time confirmation code, which the user must enter at the login prompt.
- **FIDO2 Authenticator(s)**: 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 password-less authentication to the platform 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 Question(s)**: 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 admin-defined questions available to the user. A user can create or update any available user-defined question or answer from their platform profile page.
- **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 configurations.
- **3rd Party RADIUS Authentication**: The platform communicates with the client's RADIUS server to allow for user authentication into the platform.

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.



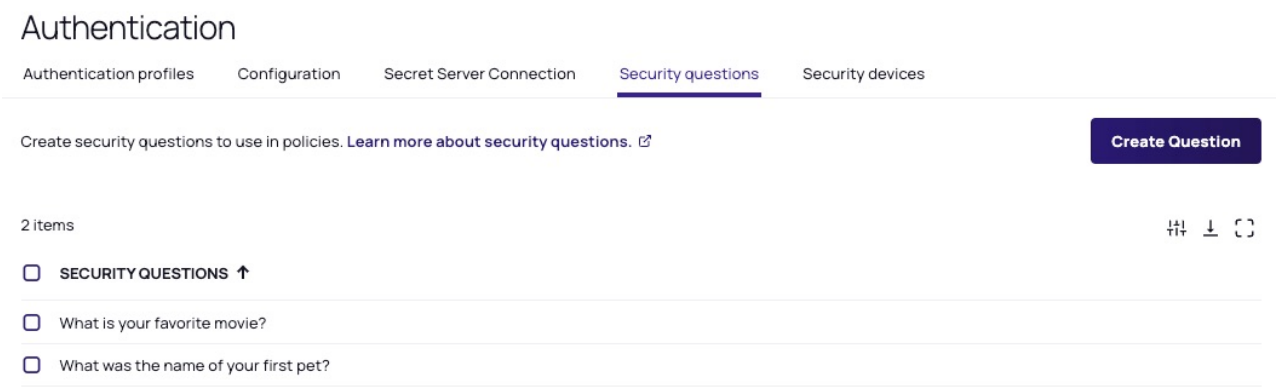
3. Click **Edit**. The page changes, enabling you to modify the settings used by MFA, such as phone numbers and email addresses. These settings include the following:

- **Authentication Parameters**:
  1. **Enable forgot username self-service at login**
     Allows users to retrieve their forgotten username. Users are prompted to enter an email address, and if the email address matches a platform account, platform sends the username to that email address.
  2. **Send email notification to users when password is changed**
     Sends an automated email after users reset 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**.

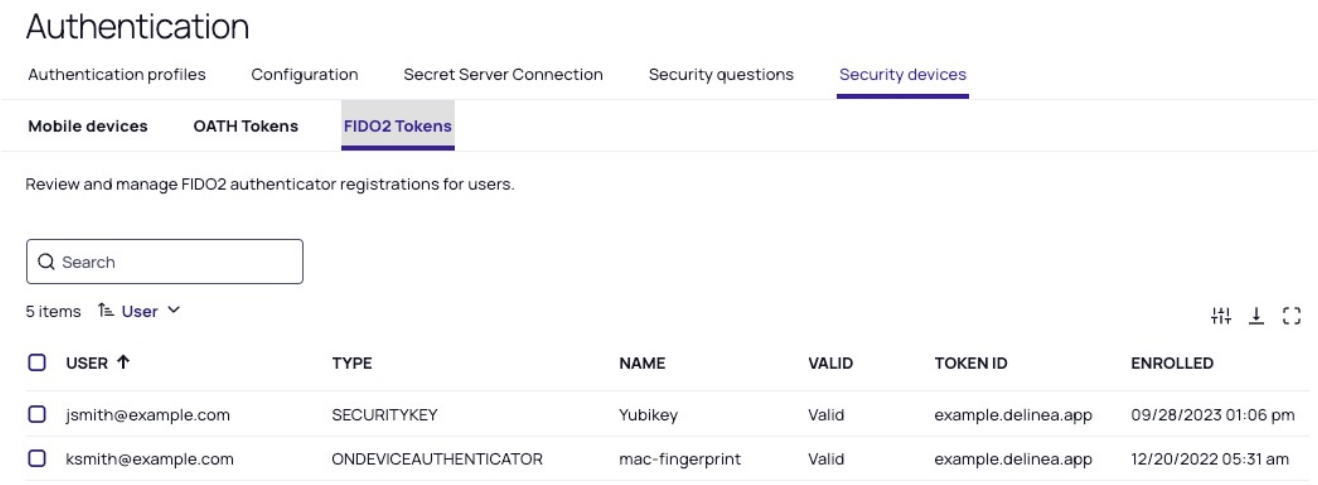


To add a security question:

1. Click **Create Question**.
2. Type a question into the text field.
3. Click **Add**.

Security Devices

Click **Settings** from the left navigation, then select **Security devices**.



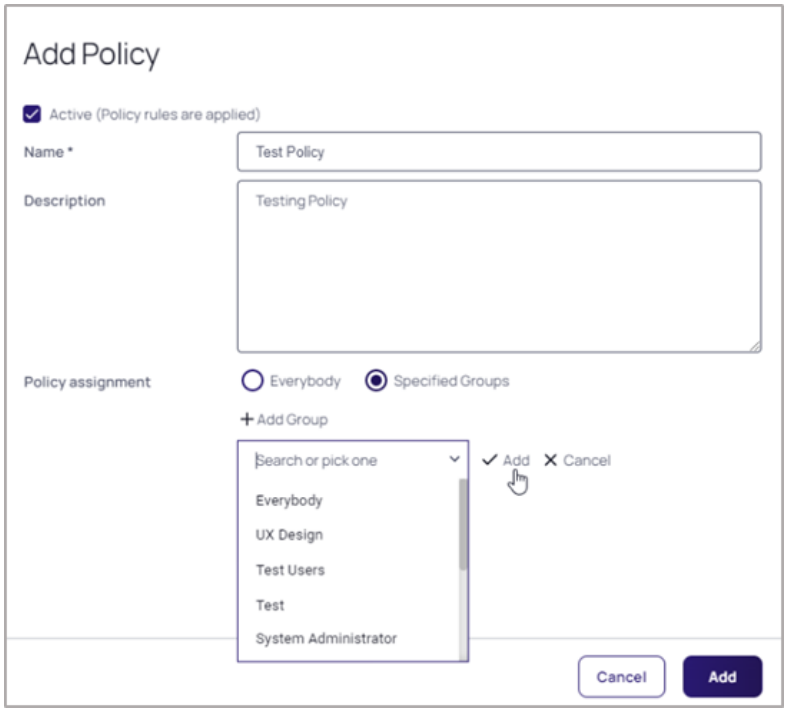
- The **Mobile devices** sub-tab displays instances of registered mobile applications with the associated users. The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. See Login Flow for the Delinea Platform Portal (MFA).
- The **OATH Tokens** sub-tab displays 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.

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 (see Identity MFA Profiles). Identity policies apply to all web logins to the Delinea Platform.

Create and Assign an Identity Policy

1. Click **Access** from the left panel, then click **Identity Policies**.
2. Click **Add Policy**.
3. Fill in the fields for:
   - **Name**: The name must be unique on the platform.
   - **Description**: The optional description should make it easy for others to identify the purpose of the policy.
4. At the top next to **Status**, select the box next to **Active (policy applied)** if you wish to activate the policy.



5. Under **Policy assignment**, choose **Specified Groups**.

   Important: If you select **Everybody**, you could lock yourself and everyone else out of the platform. Always select ***Specific Groups***, then test the policy using a test user account in a test group.

6. Click + **Add Group**.
7. Search for or select one or more groups from the drop-down list.

8. Click **Add** with the check mark before to it.
9. Click the **Add** button to create the policy.

Note: Platform will search policies for rules in stack ranked order, so set your policy order accordingly.

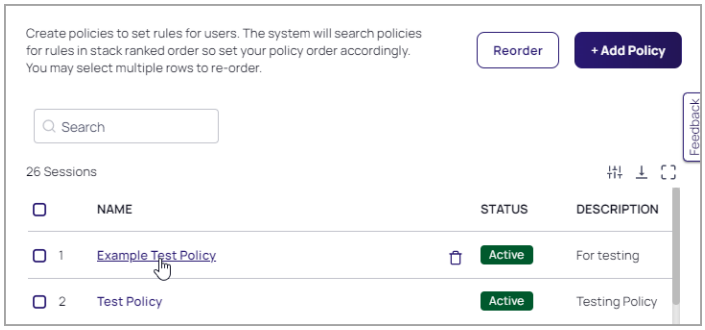
Note: For optimal policy implementation, consider assigning a new policy to a small test user group initially, before assigning it for real world use. This approach allows you to recover gracefully from issues that might arise, with minimal impact.

1. a. If you select **Everybody**, click the **Add** button to create the policy

   b. If you select **Specified Groups**:

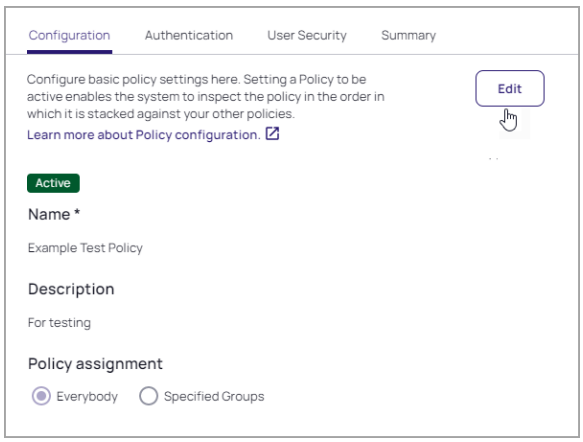
Update an Identity Policy

1. Click **Access** from the left panel, then click **Identity Policies**.
2. Click the policy you'd like to edit.

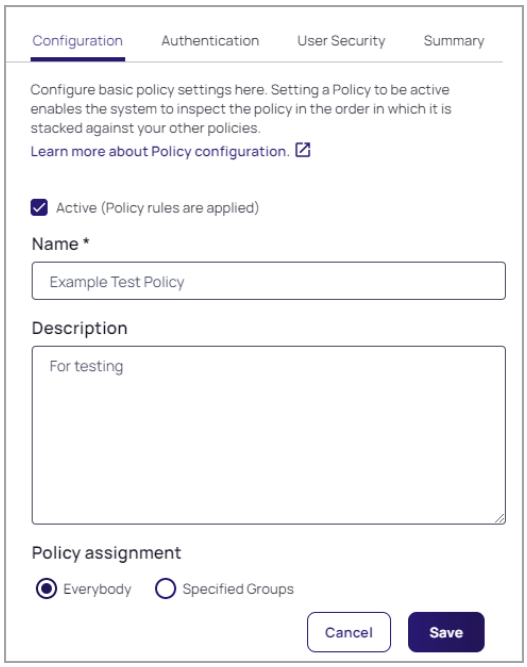


The policy page opens to the **Configuration** tab, which displays the policy status, name, description, and policy assignment.

1. Click **Edit**.



2. Make your changes to the **Name** or **Description** fields, or to **Policy assignment** settings.



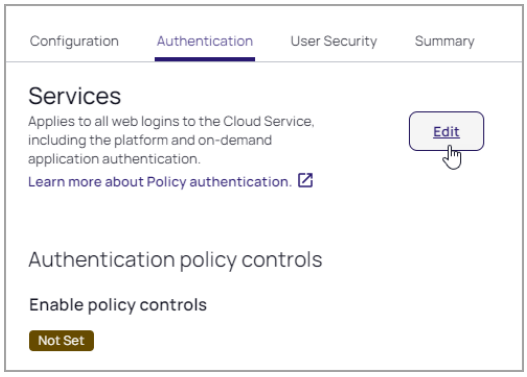
3. To assign additional groups to the policy, click **+ Add Group**.
4. Search for or select a groups from the drop-down list.
5. Click **Add** with the check mark before to it.
6. To unassign a group from the policy, click **Delete** next to the group name.
7. If you want the policy to be active, select the box next to **Active (policy applied)** if it's not selected already.
8. Click **Save**.

Authentication

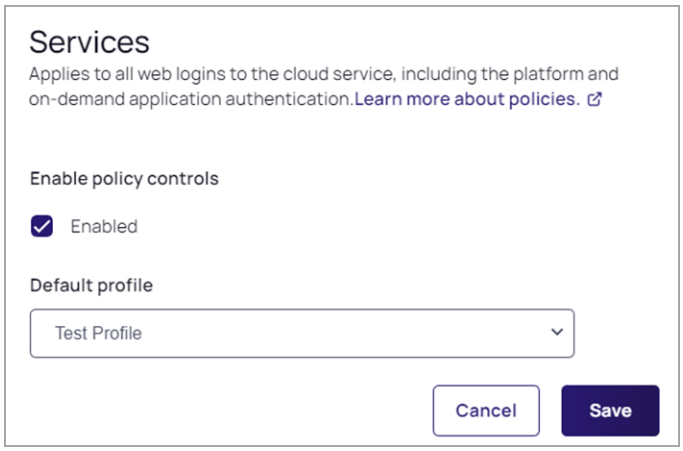
Click the **Authentication** tab. The tab displays information on the policy's Services, Authentication Rules, Browser Session Parameters, Delinea Mobile Application Session Parameters, and Other Settings.

Services

1. In the Services section, click **Edit**.



2. Under **Enable policy controls**, select **Enabled**.



3. Select a default profile from the drop-down options.

   Note: If you select **Do not allow profiles** 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 service. This can be an efficient way to restrict users from gaining access to the platform.

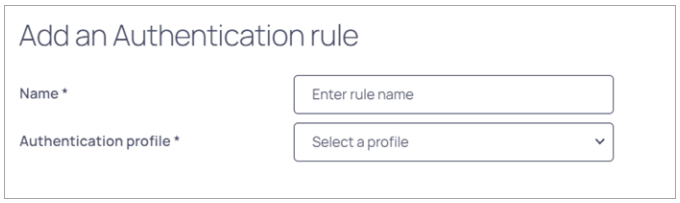
4. Click **Save**.

Once you enable authentication policy controls, you can configure the rest of the policy options on the same page.

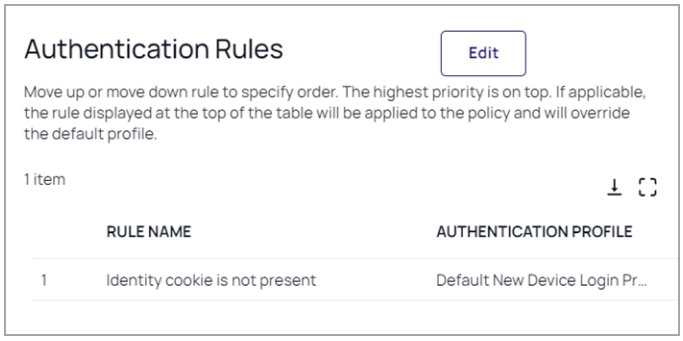
Authentication Rules

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**.
2. Click **Add rule**.



3. Enter a name for your new authentication rule.
4. Select an Authentication profile to associate with the rule.
5. Click **Add**. Your new rule now 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 uses 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 signed in' checkbox option at login (session spans browser sessions)	Enables the option to select 'Keep me signed in' at login. Persist session cookies across browser sessions. Users must select the option Keep me signed in at the login prompt to enable this capability
Session Length (in Hours)when 'Keep me signed in' option enabled	Number of hours "Keep me signed 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 = 60 minutes.

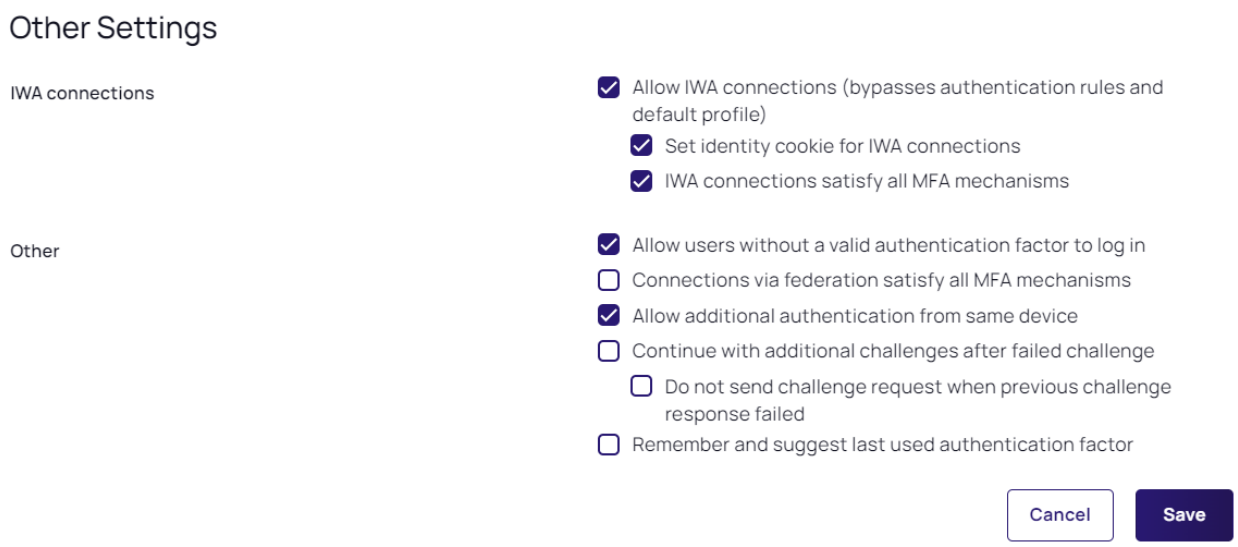
Delinea Mobile Application Session Parameters

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 mobile app. When the session length is reached, the user will have to re-authenticate with the platform. Default = 14 days, minimum value = 1 day, maximum value = 90 days

Other Settings

In the **Other Settings** section, click **Edit**.



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. Enables the use of an Integrated Windows Authentication connection as sufficient authentication for users with Active Directory accounts when they log in to the Delinea portals. 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 connector.
  - **Set identity cookie for IWA Connections**
    Enables the platform to 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 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. This option tells the platform to allow IWA to override all application-specific authentication requirements.

Other

- **Allow users without a valid authentication factor to log in**
  Exempts users from multifactor authentication when their account does not contain a mobile phone number and email address, and cannot satisfy the applied policies.
- **Connections via federation satisfy all MFA mechanisms**
  Connections using a trusted third-party federated identity provider (IdP) to log onto the Delinea Platform enable MFA on the platform through 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. When enabled, if a user is successfully authenticated via Federation, they will not be challenged with additional MFA mechanisms.

- **Allow additional authentication from same device**
  Disabling this option blocks all authentication methods to the same device except Password, Email, Security Questions, and 3rd Party RADIUS.
- **Continue with additional challenges after failed challenge**
  Notifies users of a failed authentication after the first failed challenge.
  - **Do not send challenge request when previous challenge response failed**
    Configure 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**
  To remember the last used authentication method.

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

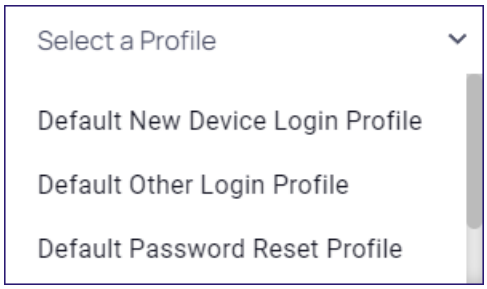
1. Click the **Self Service** sub-tab.
2. Click **Edit**, then select **Enabled**.
3. Click **Save**.

The page now displays three configuration areas:

- Password Reset
- Account Unlock
- Additional Policy Parameters

Password Reset

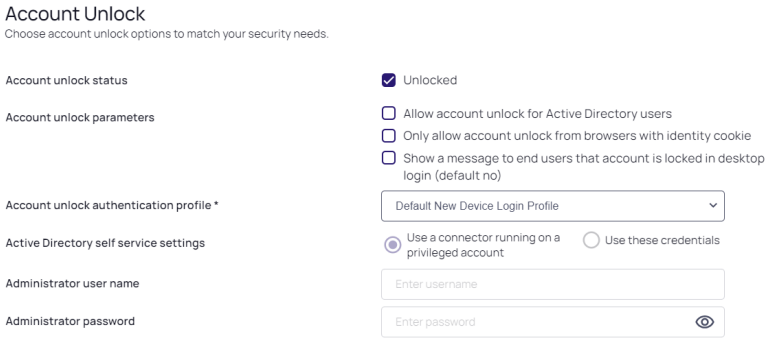
1. Click **Edit**.
2. **Password reset status**: select **Enabled**.
3. Check the boxes next to one or more of the following:
   - **Allow for Active Directory Users**
   - **Only allow from browsers with identity cookie**
   - **User must log in after successful password reset**
4. **Password reset authentication profile**: click the drop-down arrow and select a profile.



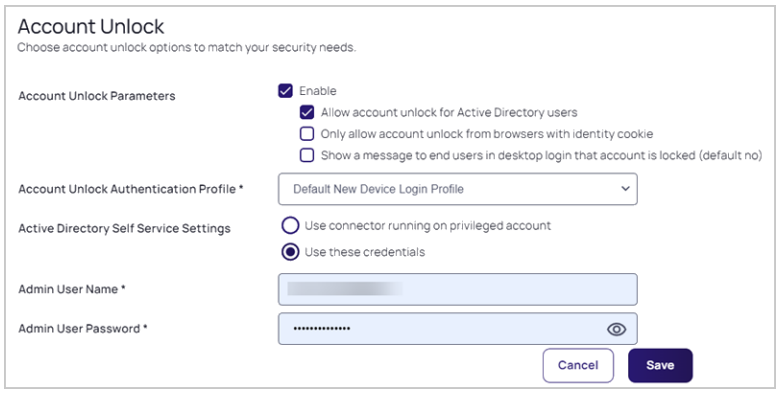
5. **Maximum consecutive password reset attempts per session**: Click the drop-down arrow to set the number of reset attempts.

Account Unlock

1. **Account unlock status**: select **Unlocked**.



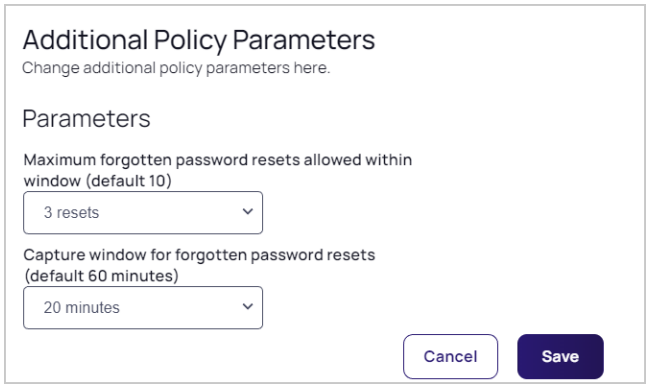
2. **Account Unlock Parameters**: Check one or more boxes next to:
   - Allow account unlock for Active Directory Users
   - Only use account unlock from browsers with identity cookie
   - Show a message to end users in desktop login that account is locked (default no)
3. **Account unlock authentication profile**: Select a profile from the drop-down.
4. If you checked the box next to **Allow account unlock for Active Directory Users**, you can choose a setting next to **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**.



6. Click **Save**.

Additional Policy Parameters

1. Click the **Edit** button.
2. Select an option from the drop-down menus for:
   - **Maximum forgotten password resets allowed within window (default 10)**
   - **Capture window for forgotten password resets (default 60 minutes)**



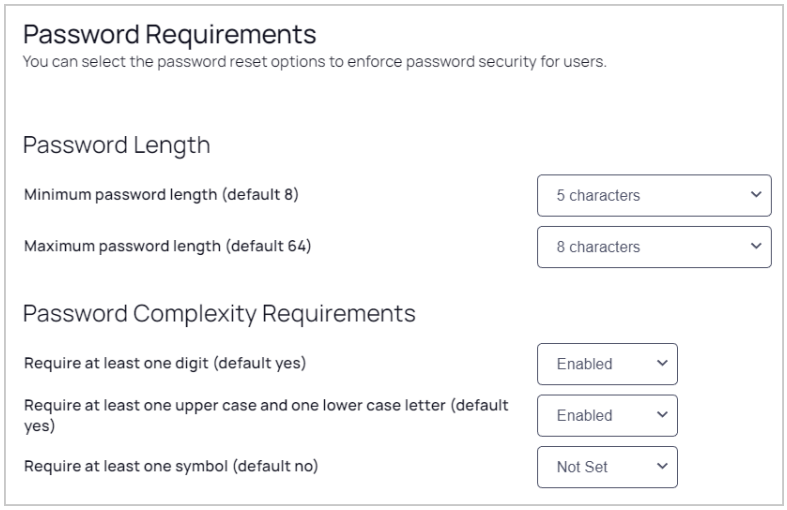
3. Click **Save**.

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

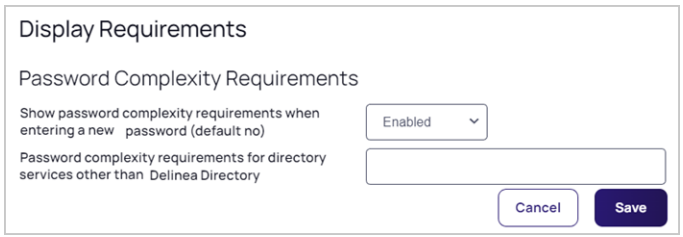
1. Click the **Edit** button.



2. Make your selections for **Password Length** and **Password Complexity Requirements**
3. Click **Save**.

Display Requirements

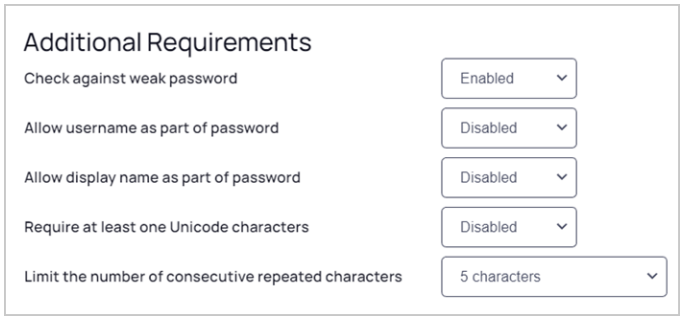
1. Click the **Edit** button.



2. Make your choices for:
   - **Show password complexity requirements when entering a new password (default no)**
   - **Password complexity requirements for directory services other than Delinea Directory**
3. Click **Save**.

Additional Settings

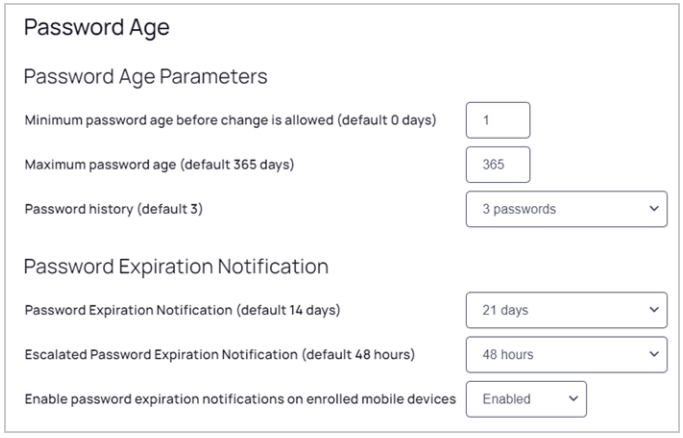
1. Click the **Edit** button.



2. Make your selections from the drop-down boxes.
3. Click **Save**.

Password Age

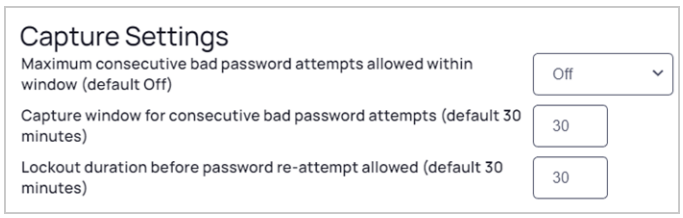
1. Click the **Edit** button.



2. Make your selections below **Password Age Parameters** and **Password Expiration Notification**.
3. Click **Save**.

Capture Settings

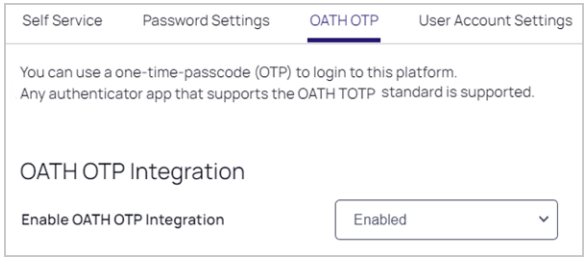
1. Click the **Edit** button.



2. Make your selections from the drop-down boxes.
3. Click **Save**.

OATH OTP

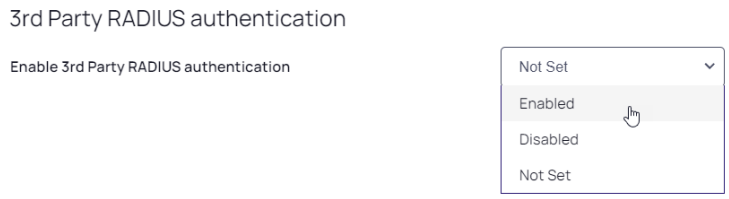
1. Click the **OATH OTP** sub-tab
2. Click the **Edit** button.



3. Select **Enabled** from the drop-down box.
4. Click **Save**.

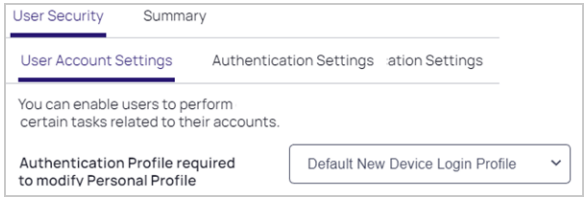
RADIUS

1. Click the **RADIUS** sub-tab
2. Enable RADIUS



User Account Settings

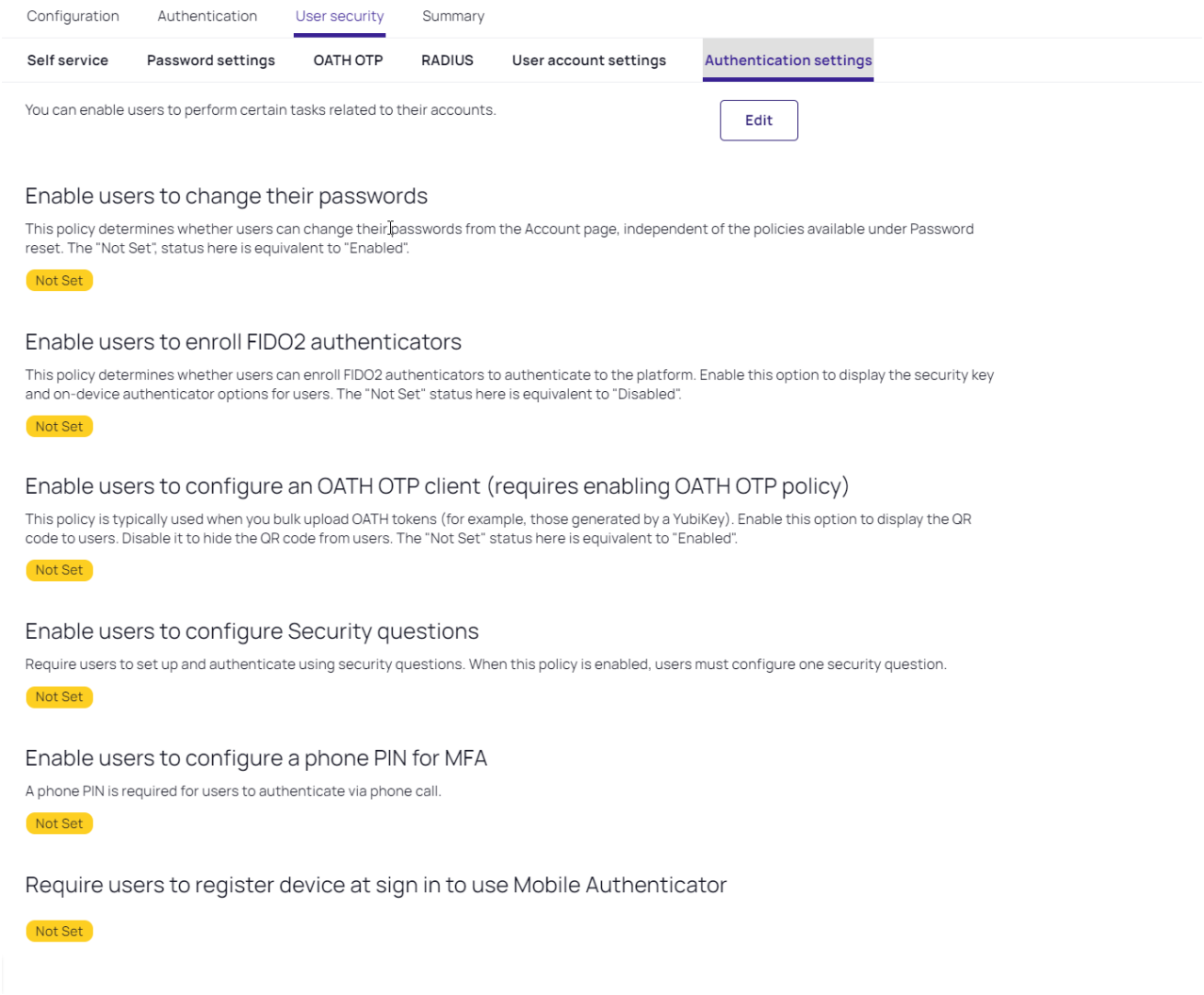
1. Click the **User Account Settings** sub-tab
2. Click the **Edit** button.



3. Make your selection from the drop-down box.
4. Click **Save**.

Authentication Settings

1. Click the **Authentication Settings** sub-tab. Each authentication setting is labeled either **Active** or **Not Set**.
2. At the top of the page next to, **You can enable users to perform certain tasks related to their accounts**, click **Edit**.



The page displays the sections listed below, and under each section heading is a drop-down 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

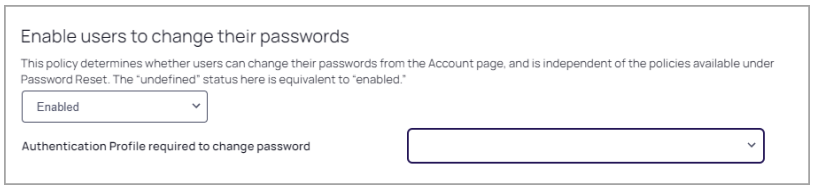
- Enable users to configure a Phone PIN for MFA
- Require users to register device at sign in to use Mobile Authenticator.

Note: The Delinea Mobile app can be used as an MFA mechanism for logging in to the Delinea Platform. See Login Flow for the Delinea Platform Portal (MFA).

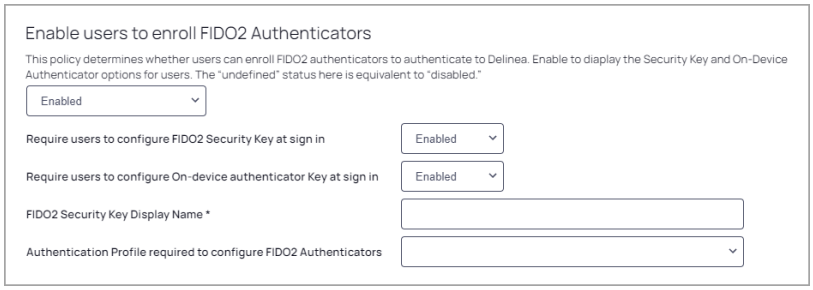
For each user capability that you enable, more fields appear where you can configure additional settings, including the authentication profile required for the user to access the capability, as shown in the images below.

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.

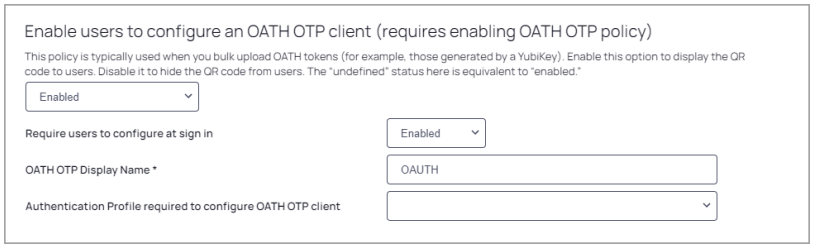
Enable users to change their passwords



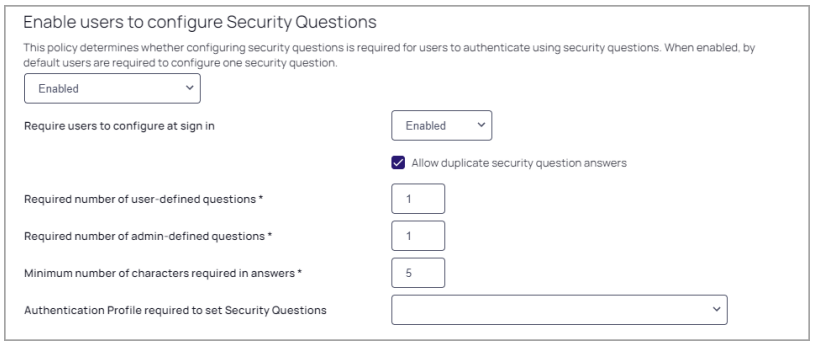
Enable users to enroll FIDO2 Authenticators



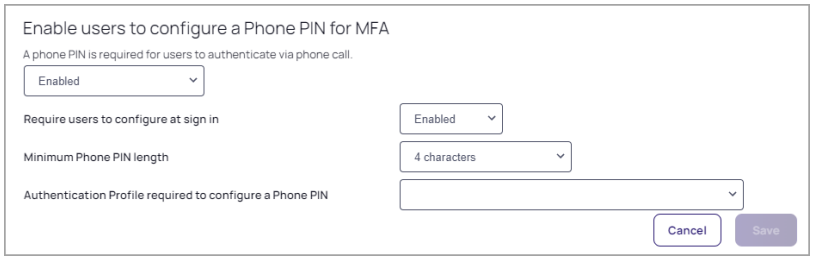
Enable users to configure an OATH OTP client



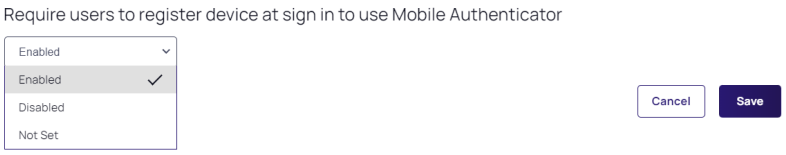
Enable users to configure Security Questions



Enable users to configure a Phone PIN for MFA



Require users to register device at sign in to use Mobile Authenticator



When you are finished making your selections, click **Save** at the bottom of the page.

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.

MFA for Secrets

Multi-factor authentication (MFA) for secrets gives 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 “out of the box.” 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 on their side. 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 Identity MFA 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. That secret's page appears.

   Note: The enabled secret in this case will inherit a default authentication profile selected on a global level.

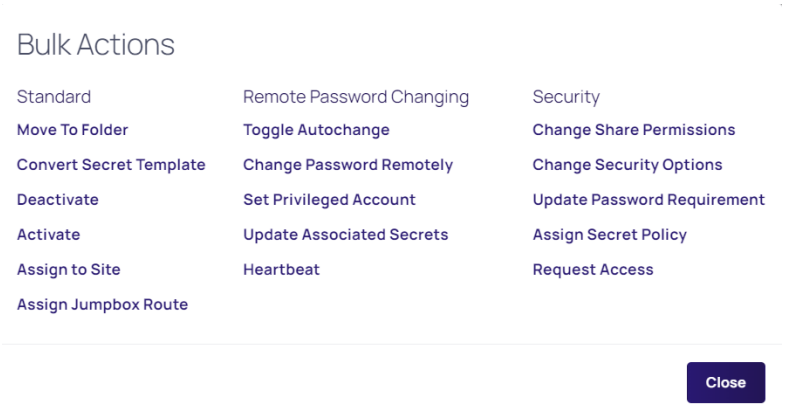
3. Select the **Security** tab.
4. In the **Multi-factor Authentication** section, click **Edit**.
5. Select the box next to **Require Multi-factor Authentication.**
6. Click **Save**.

Assign MFA to a Secret Policy

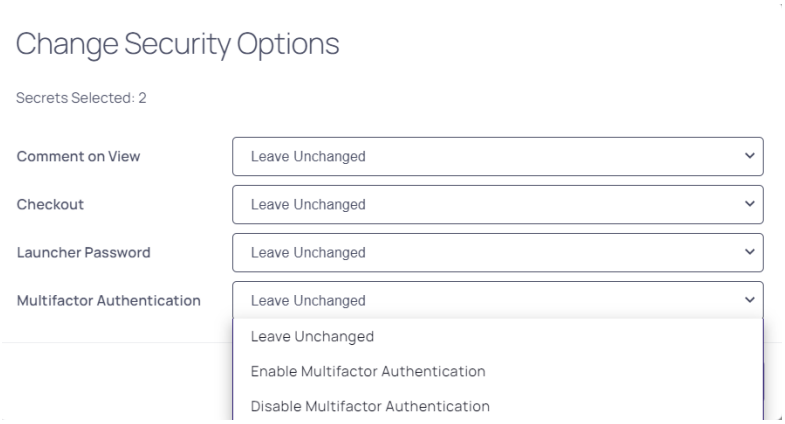
1. Click **Settings** from the left navigation, then click **Administration.**
2. Under Core Actions, click **Secret Policies**.
3. Click a policy.
4. Select the **Security** tab.
5. Click **Edit**.
6. Next to **Require Multi-factor Authentication**, select **Yes** from the drop-down.
7. Click **Save**.

Assign MFA to Secrets through a Bulk Operation

1. Click **Secret Server** from the left navigation.
2. On the All Secrets page, select the boxes next to two or more secrets.
3. In the small banner that appears, click **Bulk Actions**
4. In the **Bulk Actions** dialog under **Security**, click **Change Security Options**.



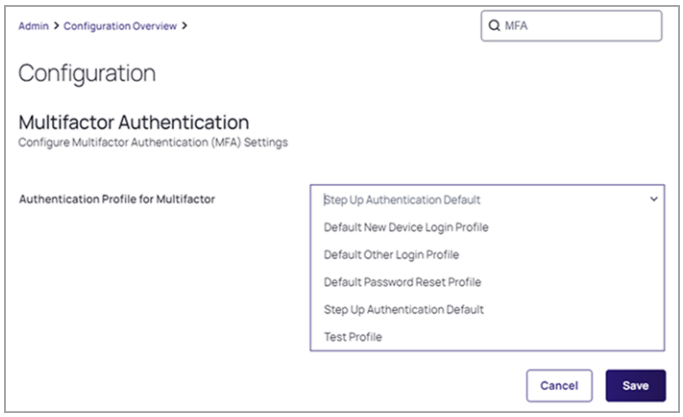
5. Next to **Multi-factor Authentication**, select **Enable Multi-factor Authentication** from the drop-down menu.



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 **Multi-factor Authentication** under Security.



3. Click **Edit**.
4. Select an MFA profile from the drop-down 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.
- During secret export, if any secret in the selected list has MFA enabled, you are prompted for MFA.
- The profile you selected for secret MFA does not impact the profile for authenticating into the Delinea Platform.
- Secret Server Cloud cannot access MFA-protected secrets unless it was itself authenticated through the platform. If not, the user is instead prompted with a link to redirect to the secret in the platform.
- MFA-enabled secrets are not available in the Secret Server mobile application.

Corporate IP Range

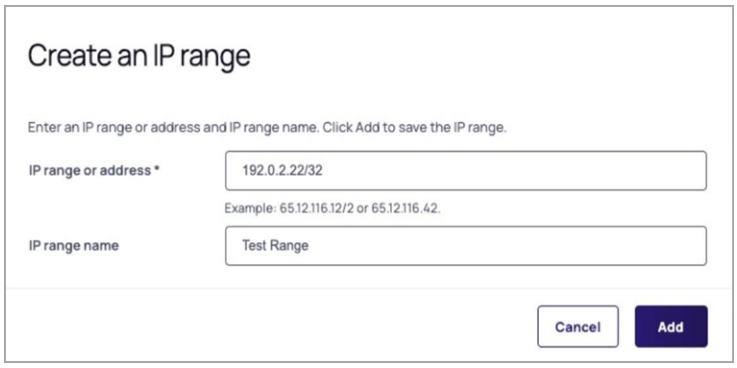
The Corporate IP Range function is used to define IP ranges for both internal and external networks, and to define authentication requirements such as the locations or IP ranges from which users can log into the Delinea Platform.

To manage corporate IP Ranges, follow the procedures below.

1. Click **Settings** from the left navigation, then select **Corporate IP Range.**

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**.



3. Click **Add** to create the new IP range.

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 delete it.
2. When prompted to confirm, click **Delete**.

RADIUS Configuration

Radius Authentication Overview

You can use your RADIUS server to authenticate users to the Delinea Platform. Enabling this requires 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.

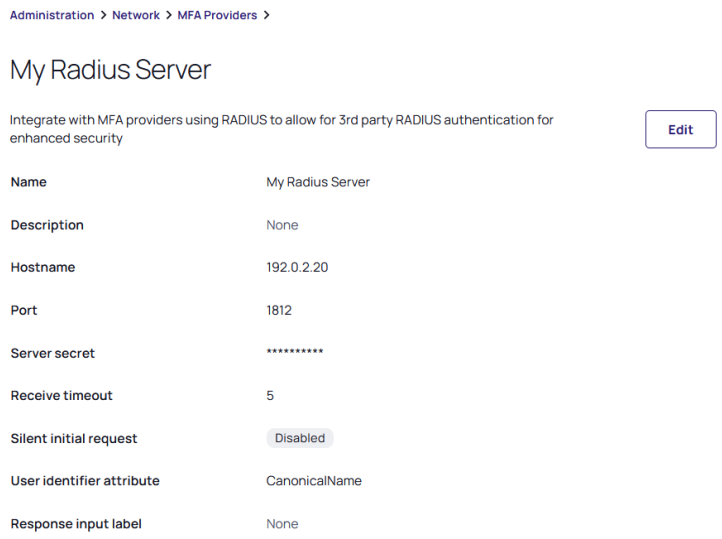
In most cases you need the following information, regardless of the RADIUS server you are using:

- 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. By default: 1812.
   - **Server Secret**: This field asks for the secret that is shared between the RADIUS Server and the platform. If you have entered a secret key on your RADIUS server, then enter that same key here. The keys must match to enable authentication. (If you are creating a new secret key, best practices recommend 22 or more characters in length).
   - **Receive Timeout (seconds)**: Enter a value to specify the receive timeout for this server. The value must be no less than 5 seconds and no greater than 55 seconds.
   - **Enable silent initial request + Silent request answer**: Enable 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 (i.e. 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 match exactly the user attribute name in the directory service. For example, you must use sAMAccountName instead of "sam account name" or "mail" instead of "Mail."

- **Response Input Label**: This sets a custom label to use for the response input during login. This field can be up to 70 characters.

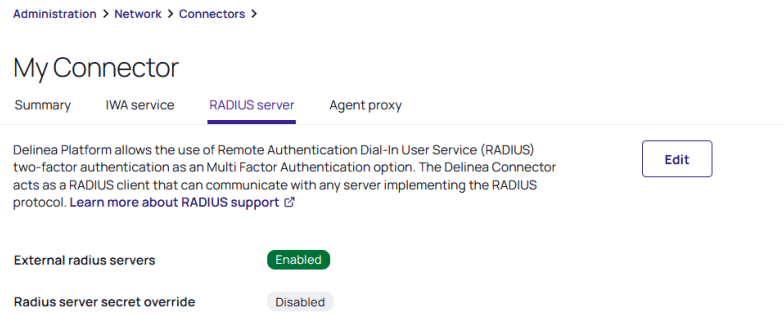


5. Click **Add Provider**.

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



4. Click **Edit**.
5. Enable the option for **External RADIUS servers**.

6. (Optional) If you do not want all your Connectors to have the same shared secret, you can override the secret here and enter a different secret. 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 "Delinea Connector" on page 34.

Using Multiple Delinea Connectors as RADIUS clients

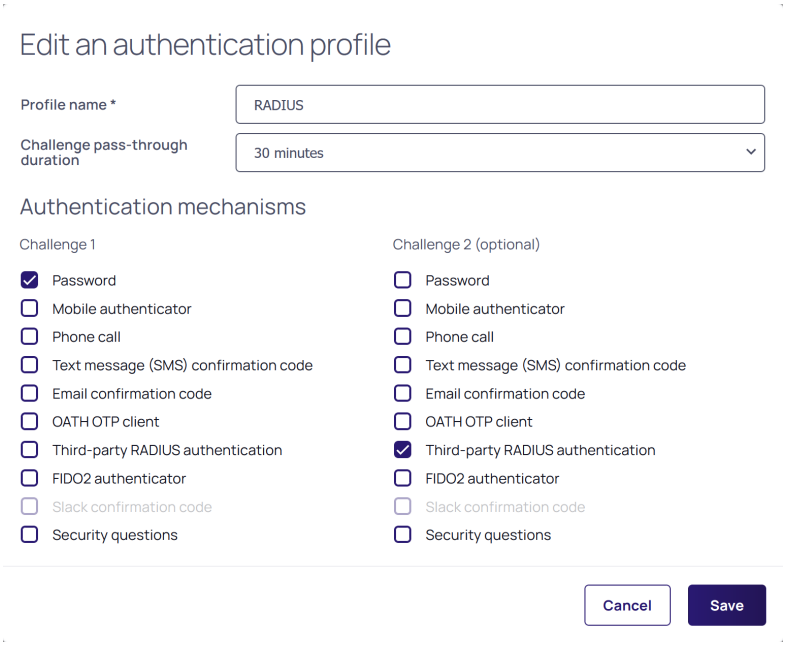
If you have multiple Delinea Connectors enabled for use as RADIUS clients, the platform prioritizes connection with them in the following order:

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**.
4. Enter a name and description.
5. **Challenge pass-through duration**: Select a duration from the drop-down options. 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.

Here's an example:

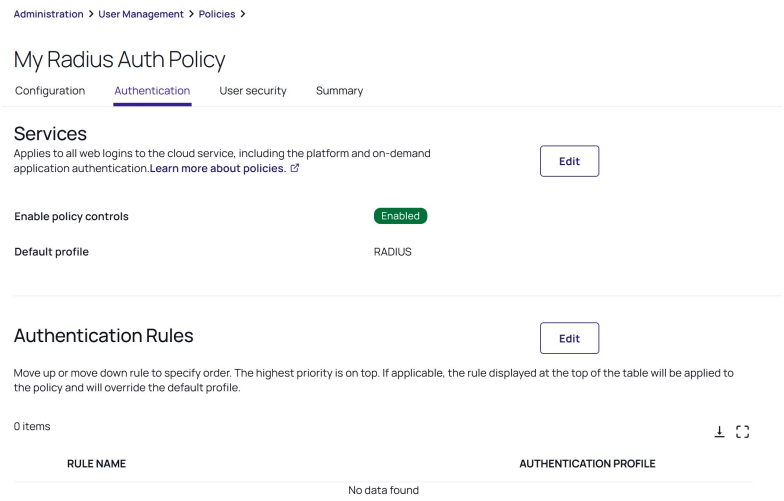


Configure a RADIUS Identity Policy

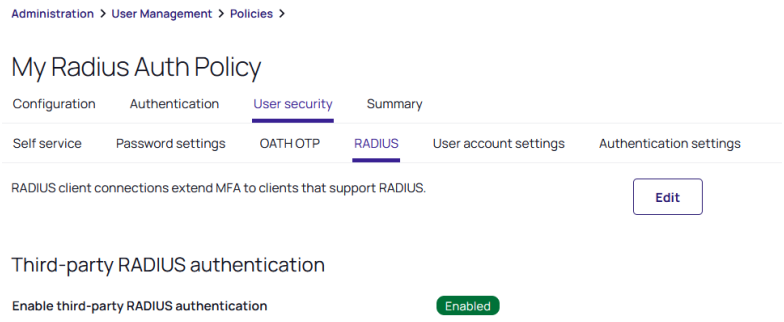
You also need to configure an identity policy to control who can log in using RADIUS and how they must do so.

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. **Enable authentication policy controls**: Select **Enabled**.
6. **Default authentication profile**: Select the authentication profile you created earlier for RADIUS from the drop-down.

   For example:



7. Select the **User Security** tab.
8. Select the **RADIUS** sub-tab.
9. Click **Edit**.
10. **Enable 3rd Party RADIUS authentication**: Select **Enabled**.
11. Click **Save**.

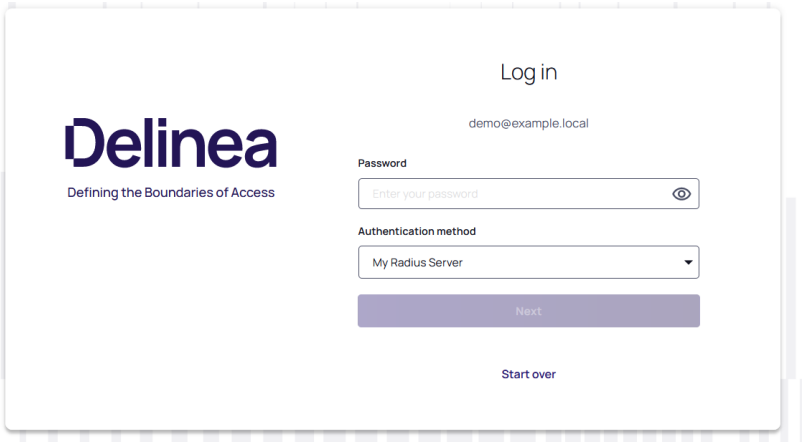


Using RADIUS Authentication

Users can access the Delinea Platform by opting for the RADIUS server authentication challenge method at the platform login prompt and subsequently entering the passcode.

Important: The passcode requirements may vary based on the specific authentication backend employed by the RADIUS server.

For example, here's what it looks like at login when the service prompts a user to authenticate against the RADIUS server:



IWA Configuration

The Delinea Platform enables you to accept an Integrated Windows Authentication (IWA) connection as sufficient authentication for users with Active Directory accounts when they log in to the Delinea portals. 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 connector.

If you have multiple connectors enabled for IWA, the platform prioritizes connection to them using the following workflow:

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, and that connector must be joined to Active Directory in the forest to which users are authenticating.
- Decide if you want to:
  - Use a certificate from a trusted external certificate authority (CA) such as Symantec or GoDaddy.
  - 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 option may be as good as, or better (depending on the company infrastructure) than 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)

Enabling IWA Service on the 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.
   You can modify the following settings:

Setting or property	Change to do the following
Enable web server	The default value is Enabled. This setting supports 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 connector's host computer's name. You can enter a DNS short name here or the fully qualified domain name in the IE local intranet zone.
IWA Detection Timeout	The length of time IWA will wait for response from the connector. The default is 10 seconds.
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	c

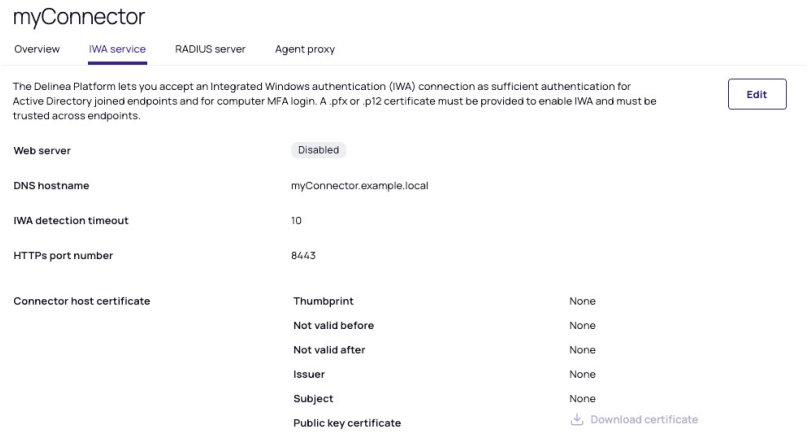
3. Click **Save**.
4. Click **Settings**.
5. Click **Corporate IP Range**.
6. Click **Add** to enter your corporate IP range. IWA will not work for users whose computers are outside of the defined corporate IP range.
7. Click **OK**.
8. Reboot your Delinea Connector if you have uploaded a certificate.

Importing a Certificate

If you are using internal or third-party CAs, you need to import those certificates onto the platform. You can import wild card certificates.

To import a certificate onto the platform:

1. From the left navigation menu, click **Settings** then click **Connectors** from the secondary menu.
2. Select the relevant connector.
3. Click **IWA Service** on the Delinea Connector Configuration page.
4. Confirm that the box next to **Enable Web Server** is selected.
5. Click the **Upload** button to import an internal or third-party certificate. You can upload the same certificate to all Delinea Connectors in the same domain. If you do this, make sure you upload the same certificate to all IWA configured connectors. Ensure the subject of the certificate explicitly matches the hostname of the connector, or matches via a wildcard in the subject.
6. Navigate to your CA and upload it. Enter the password protecting the certificate if required.
7. Click **Save**.
8. You must restart the Delinea Connector after importing the certificate.



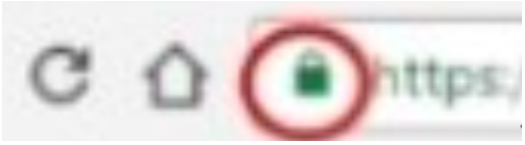
Certificate Metadata:

- **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 easily download the public key certificate for distribution to your endpoints.

Verifying IWA Over HTTPS

You can test the validity of the Delinea Connector host certificate by doing the following:

1. Open a web browser from an endpoint machine
2. Navigate to the following address: https://<yourconnectorhostname>:<httpsport>/iwa/ping.
3. Replace <YourConnectorHostname> and <httpsport> with the corresponding values. For example: https://2008WindowsServer:8443/iwa/ping
4. Look for the green certificate icon in the browser.



Enabling IWA in the Authentication Policy

You can configure the platform to bypass already configured authentication rules and default authentication profiles when IWA is configured. This option is configured by default.

To enable IWA in the authentication policy:

1. Log in to Admin Portal.
2. Click **Access** from the left navigation, then select **Identity Policies.**
3. Click an identity policy to open it.
4. Select the **Authentication** tab.
5. Scroll down to Other Settings and select the box next to **Allow IWA Connections** (bypasses authentication rules and default profile).
6. Scroll up to the Services section.
7. Click **Edit**.
8. Select a default authentication profile from the **Default Profile** drop-down, for the platform to use if IWA is not available and other authentication conditions are not met.
9. See Identity MFA Profiles for more information on authentication profiles.
10. 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 log in. The platform checks the browser for this cookie when the user logs in to the Admin Portal. As long as the cookie is there, the user is not prompted for multi-factor authentication.

To use IWA with identity cookie:

1. 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 box next to **Set identity cookie for IWA connections**. 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

This is an optional configuration. You can configure the platform to use IWA to override all application specific authentication requirements. For example, you can configure the Box application to require two authentication challenges if users are accessing the application from inside the network. However, you can tell the platform to ignore those authentication requirements if IWA is available.

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 box next to **IWA connections satisfy all MFA mechanisms.** This option tells the platform to allow 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. Select the relevant connector.
3. Deselect the **Enable Web Server** option.
4. Click **OK**.

Mobile Access

Most functions pertaining 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 an overview of the functions available for the Delinea Mobile application, see the Delinea Mobile Overview.

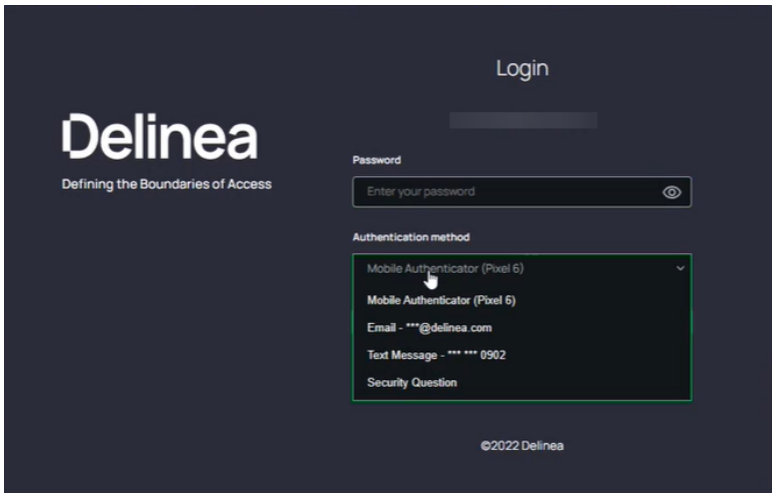
Administrators

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**.

Administrators can also make MFA a login option for users of Delinea Mobile. See Authentication Profiles and MFA.

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 via mobile device, the user will see each of their registered mobile devices on the login screen under **Authentication Method**, with the device name in parentheses after **Mobile Authenticator**.



Platform Notifications

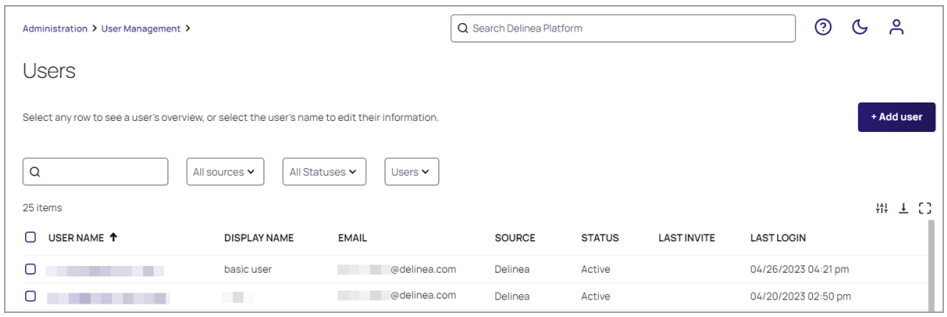
To receive notifications from the platform on a mobile device, a user must first log into the platform at least once from the device. This first login registers the user's mobile device to the user's profile. The user can then receive and reply to notifications such as login MFA challenges even when they are not logged into the mobile application.

A device can be registered to only one platform user profile at a time. If a different user subsequently logs into the same platform tenant from the same registered device, the device will be deregistered from the original user's profile, and the original user will no longer able to receive notifications from the platform.

If a user no longer wishes to receive notifications on a device, they must log into their platform tenant, go to their profile, and delete the device from their list of registered devices.

User Management

To view users on the platform, click **Access** from the left navigation, then select **Users**. The Users page displays all users on the platform, including Active Directory, Federated, and local users. For each user, the page displays the user name, display name, email address, source, status, last invite, and last login.



Click a **User Name** to go to that specific user page, where you can view and edit many settings for the user account, including the user's group memberships, roles, policies, activities, and attributes.

See Adding Users for instructions on adding users to the platform.

See Managing Users for instructions on managing platform users.

Avoid Adding Local Users

Users should be added to the platform only through federation or through their memberships in Active Directories. Adding local users to the platform is not considered a best practice for privileged access management, for the reasons explained below.

Typically, the 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.

If local user accounts are ever added, they should be added ***very rarely***. For example, you might need to add a very temporary local user account for someone who needs to try out platform functionality.

Note: Local accounts cannot be converted to domain accounts.

Note: After setting up the Connector on the platform and adding Active Directory users, do not add an existing Secret Server user as a platform local user, because doing so could cause synchronization issues between the platform and Secret Server.

Adding Users

Adding a Local User Account

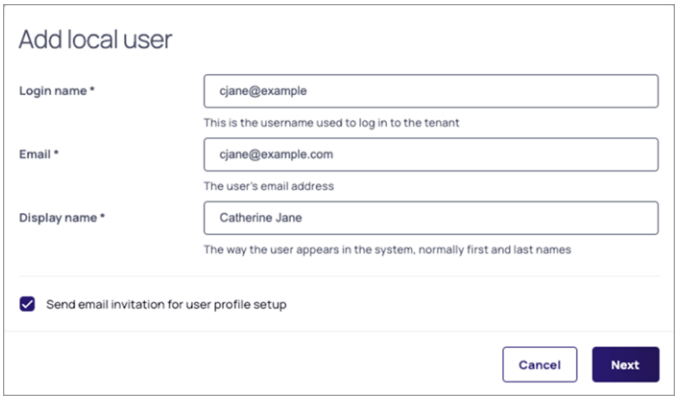
Adding local user accounts is not considered a best practice for privileged access management and typically should be used ***very rarely***. For example, you might need to add a local user account for someone who needs to try out platform functionality for a very limited time. We recommend leveraging Active Directory or Federation to grant users access to the platform.

Notes:

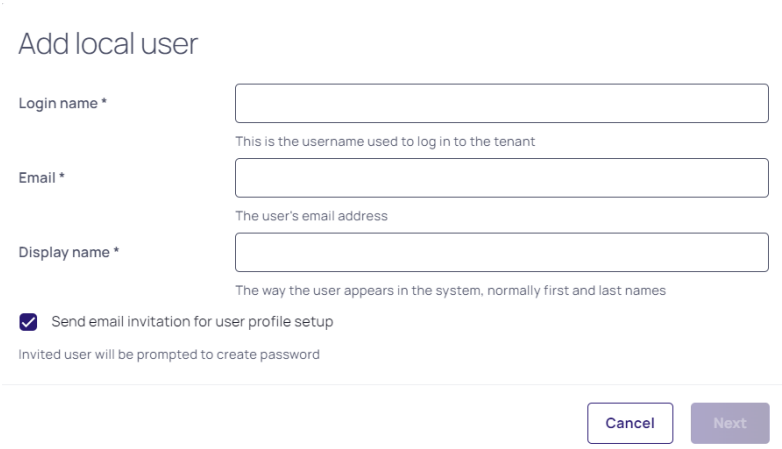
- Local accounts cannot be converted to domain accounts.
- After the Connector is installed and Active Directory is set up on the platform, do not add an existing SSC user as a local user, because doing so could cause synchronization issues between the platform and Secret Server.

To Add a New Local User

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**



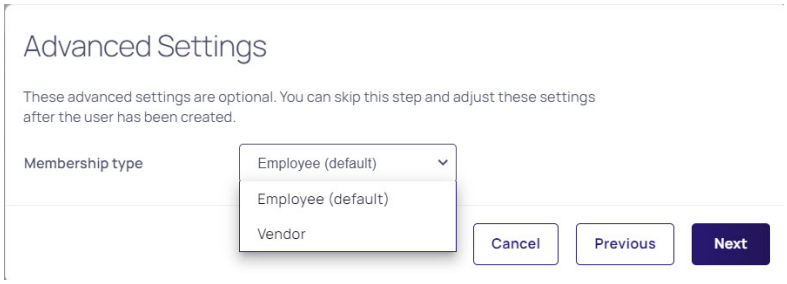
The field, **Send email invitation for user profile setup** is selected by default. If you leave this option selected, the user will automatically receive an email containing an **Accept** button, with a one-time password embedded in the button. When the user clicks the button, they are taken to the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



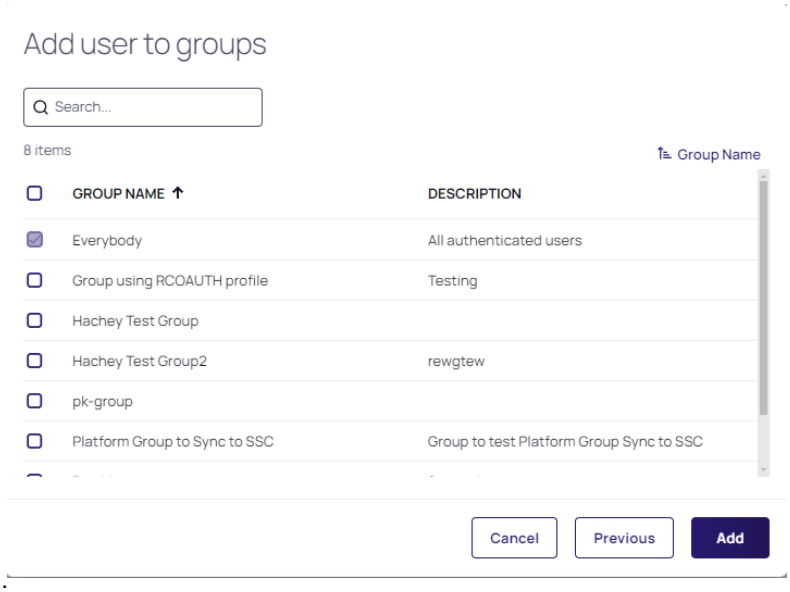
If you choose to deselect, **Send email invitation for user profile setup**, a panel opens where you can set a password for the user either manually or automatically. The user will not receive an email invitation to log into platform in this case, and you will need to copy and save the password and deliver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

5. Click **Next**
6. The Advanced Settings window appears. Please note, that the default **Membership Type** will be set to *Employee.* This can later be changed to *Vendor* .See "Advanced Settings " on page 197for more information. Click **Next** after you have selected the correct membership type.

   Important: This functionality is currently available only to customers participating in the private preview. If you'd like to participate to be among the first to try this functionality, ask our support or account team for details



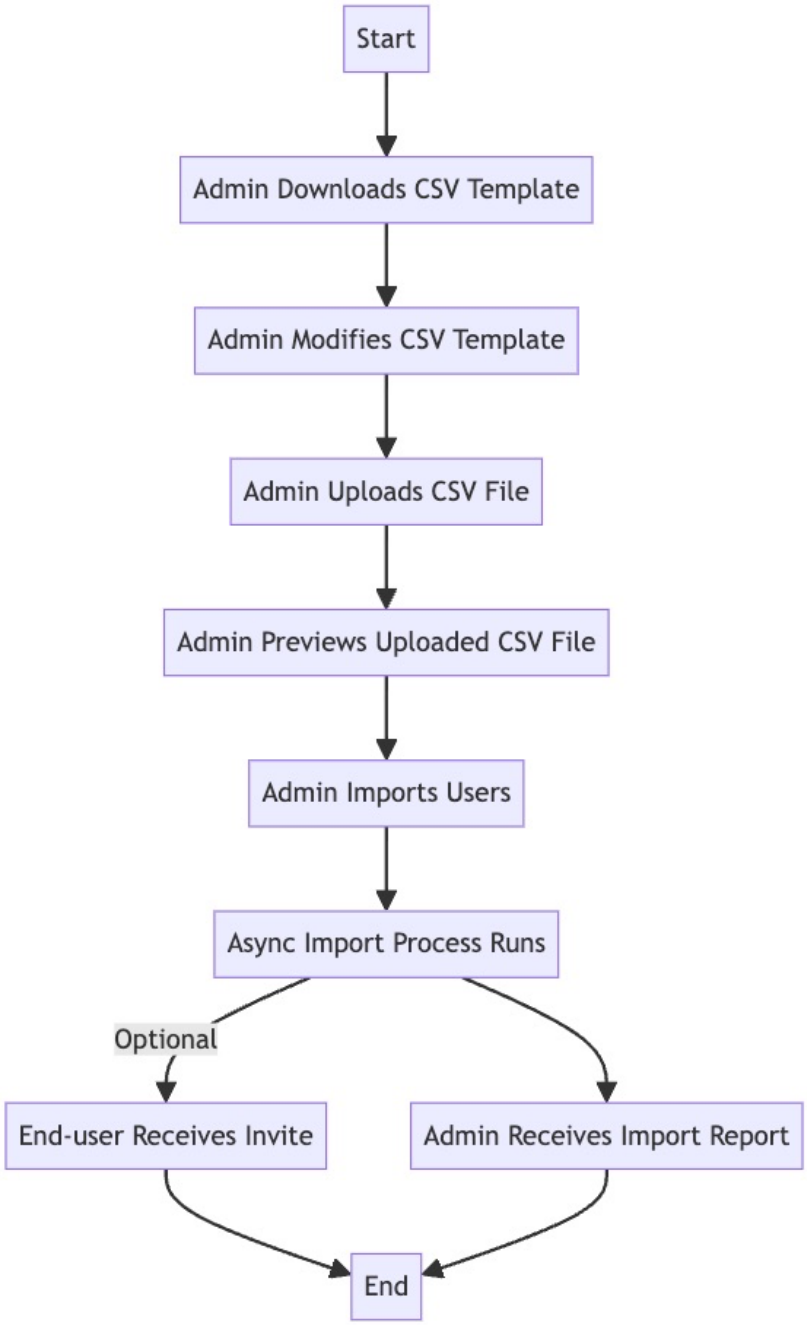
7. Add the new user to a group, if needed.



Bulk Import Local User Accounts

The bulk import feature streamlines the process by enabling administrators to import a large number of user accounts 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.

Workflow:



Steps:

1. Log into the platform
2. Click Access from the left navigation, then select Users.
3. Once in the Users section, locate and click on the Import Users button.
4. Download the provided CSV template by clicking on the respective option.

5. Open the downloaded CSV template and update it with the necessary user account information you wish to add. Refer to the guidelines provided below for guidance.
   - All required fields must be present.
   - Each field must have a header.
   - Headers must match exactly as shown in the following table, including upper case characters and spaces.
   - Fields/Attributes not listed in the following table must be defined in **Settings** > **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 exist already.
Email Address	**Required** - You can specify one email address only. The email address must be of a valid form. Plain text strings, such as “N/A” or “unavailable”, will be rejected.
Display Name	**Optional** - However strongly recommended. You can enter the display name in Excel using either format: first last last, first If you are editing the CSV file, use quotes if you specify the last name first (for example, “last, first”).
Description	**Optional** - Do not use punctuation. The limit is 128 characters.
Office Number Mobile number Home number	**Optional** - You must enter the area code. You can enter domestic US numbers in the following forms: 1234567890 123-456-7890 Use E.164 number formatting to enter an international number. If you use the phone or text message options for multifactor authentication, the Office and/or Mobile numbers must be accurate or the user cannot log in.
Groups	**Optional** - All accounts are automatically added to the Everybody role. You can specify multiple groups. Use a comma to separate each group. 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.
Expiration Date	**Optional** - Enter a date when the account expires. If you do not set a date, the account does not expire. This field is not in the CSV template.

Default Fields	Rules
Password	**Optional** - Sets the password for the user. Password requirement is based on the password policy settings in Access > Identity Policies > [User] > User security > Password settings.

Require Password Change	**Optional** - Specifies if users must change the password upon the first successful login. The supported inputs are:
	`False, f, no, n -- No password change required`
	`True, t, yes, y -- Password change required`

Platform User Membership Type	**Optional** - By default, the membership type will be *Employee*. If you are adding vendors, be sure to change the membership type to *Vendor*. **Important:** This functionality is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this functionality, ask our support or account team for details.
Reports to	**Optional** - Name of the reporting manager. This field is not in the CSV template.

6. 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.
7. Proceed by clicking **Next** .
8. Review the first 15 records displayed in the preview. Use this opportunity to ensure that the entries are correctly formatted.
9. Once reviewed, click **Next** to proceed.
10. 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.
11. Finally, click the **Import** button to initiate the import of the user accounts

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 account if the "Send email invite for user profile setup" option was chosen. This email contains a platform link that directs users to the platform portal, where they can set up a new password unless configured otherwise.

Granting Access to User Accounts From External Directories

User accounts from external sources such as AD or Federation are added to the platform "on-the-fly" when they log in, as long as they satisfy the authentication requirements through an external source. 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 into 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 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.

On the Delinea Platform, non-local groups are *mapped*, *not added* to named platform groups.

Adding Active Directory User Accounts

To connect the platform with Active Directory, you must use the Delinea Connector. For complete instructions on downloading, installing and registering the Connector, see The Delinea Connector.

Adding Federated User Accounts

To integrate the platform with federation Identity Providers (IdPs) on the Delinea Platform, see Federation.

Note: When you add a user to a platform group that is synched to a Secret Server group, you might not see the user in the Secret Server group right away. See "Cannot See a New Platform Group User in Secret Server" on page 12.

Note: When you click **Access** from the left navigation then select **Users**, you might not see Active Directory users and groups that have been set up in Secret Server. See "Cannot See Secret Server AD Groups or Users in Secret Server" on page 13.

Managing Users

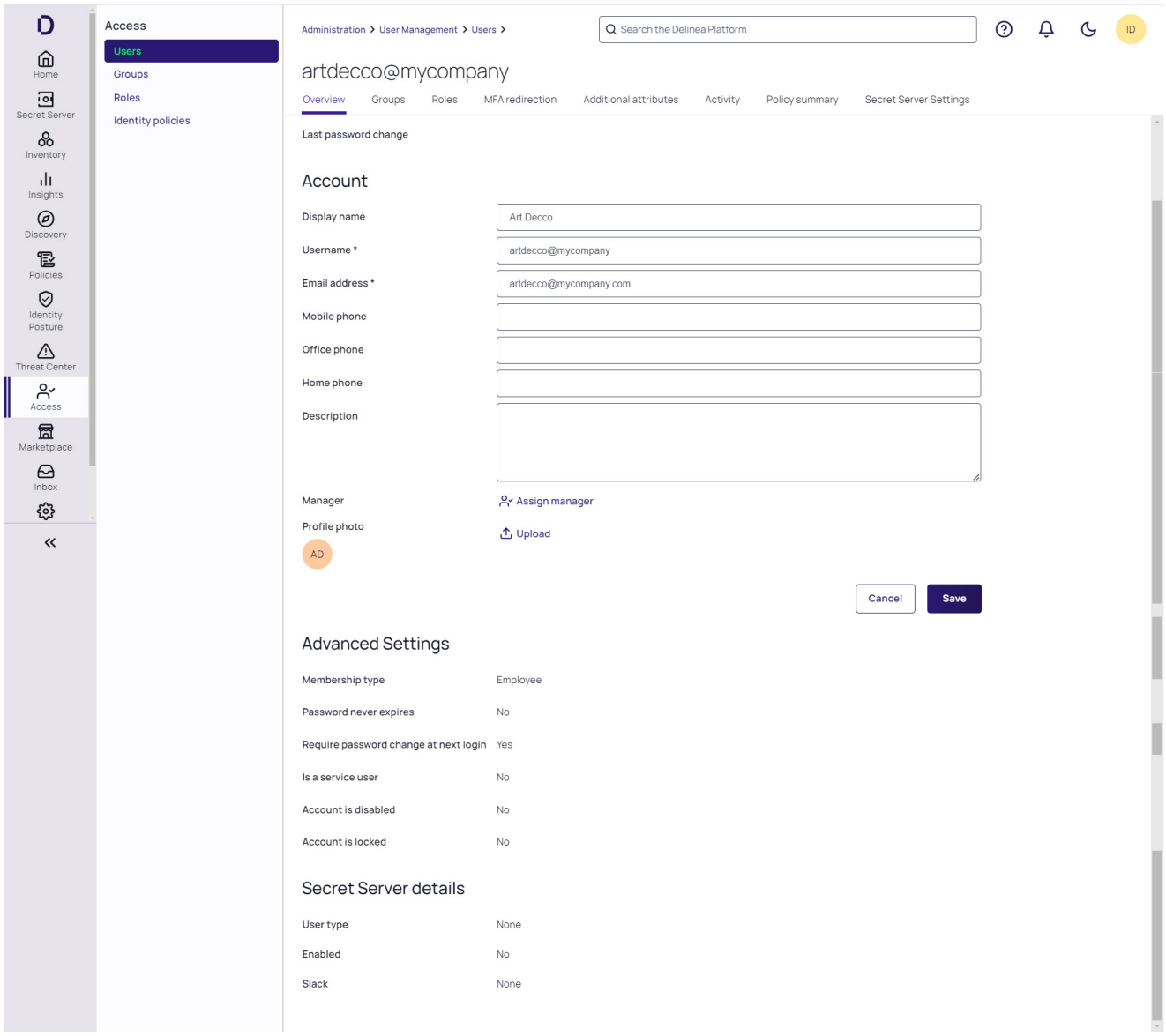
Note: Only **local** Platform user accounts can be modified as described in this section. To modify Active Directory user accounts, you must use Active Directory.

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 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.

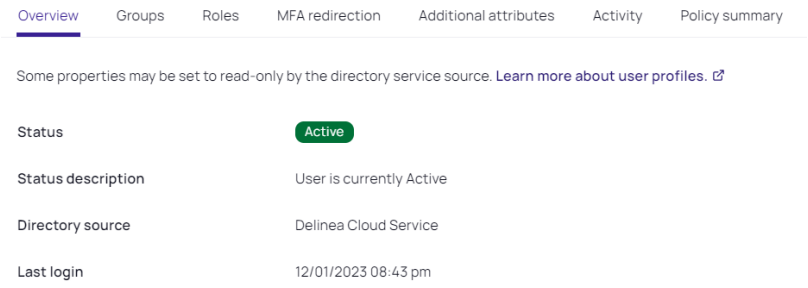
Overview

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



Important: The *Membership Type* functionality is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this functionality, ask our support or account team for details.

The top of the Overview tab displays the user's basic information, including their status, the status description, their directory source, and their last login.



Status

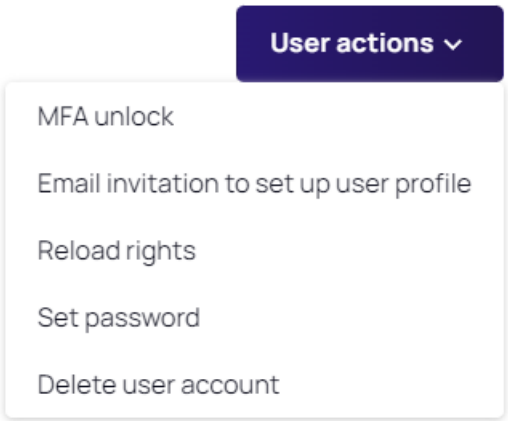
The table below provides descriptions of each status that can apply to a user.

Status	Description
Active	The user has logged in to Platform portal.
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. Upon accepting 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	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 log-in attempts. Users can be auto-suspended due to multiple concurrent password failures. In that case: - Users are auto-suspended for a duration of 30 minutes - Default Admin account (cloudadmin@< tenant >) can also be suspended for the same reason; however, the auto-suspension only lasts 5 minutes. - Continuing with the wrong password will extend the suspension. Auto suspension will end after the user logs in successfully. - The **Users** tab will continue to show as suspended (even after 5 or 30 minutes) until the suspended user logs in successfully.

User Actions

At the top right of the Overview tab, click the **User Actions** drop-down to access quick actions.



The user actions available are described in the table below.

Action	Description
MFA Unlock	Suspends multi-factor authentication for 10 minutes. Multi-factor authentication requires users to perform additional steps (such as verify their identity by email or phone call) to log in to the Platform Portal. If the user is having trouble logging in, select the user and select this action to let the user log in with just a login name and password.
Send email invite for user profile setup	Sends an email to the selected user. As part of this workflow, the user will need to change their password the next time they log in.
Reload Rights	Updates the user's rights immediately to put into effect any changes you have made to the account, for example, if you added the user to a new role or changed the user's administrative privileges. Use this action immediately after modifying the user's role or rights.
Set Password	Prompts you to reset their account password. In the window that appears, you enter a new password for the user.
Delete user account	Deletes the account from the Platform. The user will no longer be listed on the Users page and will no longer be able to log in to the Platform. For Active Directory user accounts, the deleted account is only removed from the Users page. You must use Active Directory Users and Computers to delete the Active Directory account.

Account

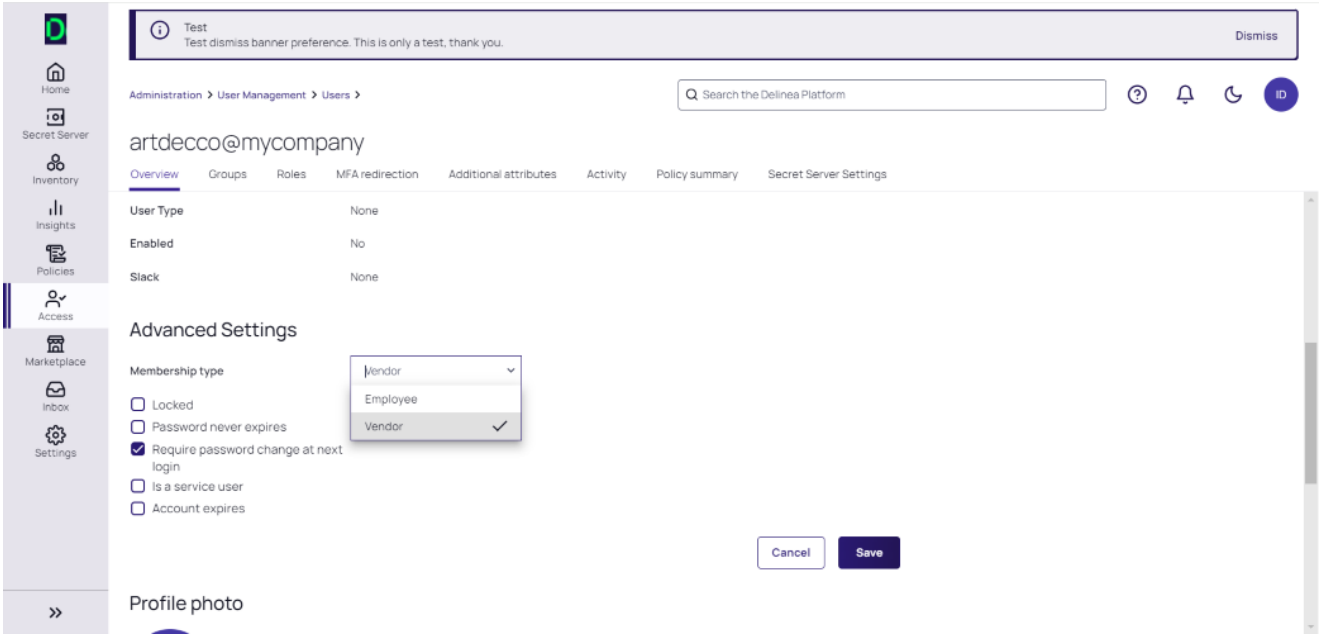
In the **Account** section, click **Edit** to modify the attributes described in the table below.

Field	Description
Login Name	The login name used to log in to the tenant. Users log in with `<Login Name>@<domain>`. For example, `jsmith@acme` or `jsmith@acme.com`.
Email Address	The email address for the user.
Display Name	The name visible to users once they are logged in to the tenant.

Advanced Settings

Important: This functionality is currently available only to customers participating in the private preview. If you'd like to participate to be among the first to try this functionality, ask our support or account team for details

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



Status

In the **Status** section, click **Edit** to select an account status as described in the table below.

Action	Description
Locked	Locks the user's account. When locked, users are prevented further access to Platform services but 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 and under**Password Setting**, set **Maximum consecutive bad password attempts allowed**. **Note**: The default admin account (cloud@< tenant >) cannot be manually locked. For this account, the option will be grayed out.
Password never expires	Overrides the default "Maximum password age" identity policy setting. Regardless of the "Maximum password age" setting, the password for this account never expires. **Note**: This setting and the "Require password change at next login" setting are interdependent. If you select one, the other is reset.
Require password change at next login	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. **Note**: This setting and the "Password never expires" setting are interdependent. If you select one, the other is reset.
Is Service User	Select this option for service users - non-interactive users. These users will not belong to the Everybody role.

Secret Server details

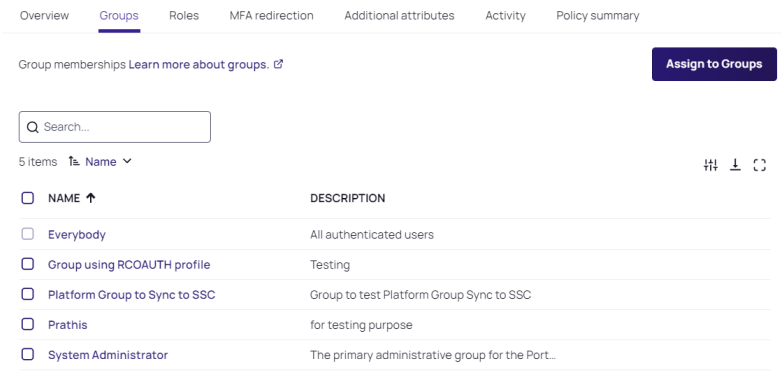
User types:

- **Hybrid** users have direct access to both the platform and Secret Server. Passwords are not synchronized between the platform and Secret Server, requiring users to reset their passwords independently in platform and/or Secret Server.
- **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

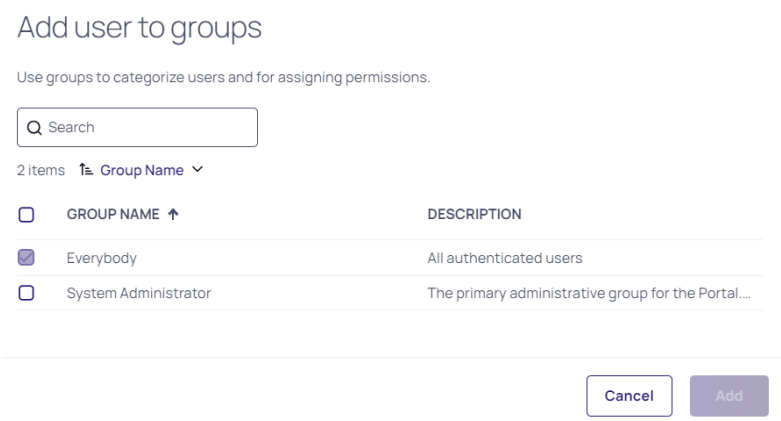
Groups

An administrator can manage group membership for users two ways: from the Groups view or from an individual User view. See Group Management for more information

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 To Groups**.
3. Select one or more groups.
4. Click **Add** to add the user to the groups selected.

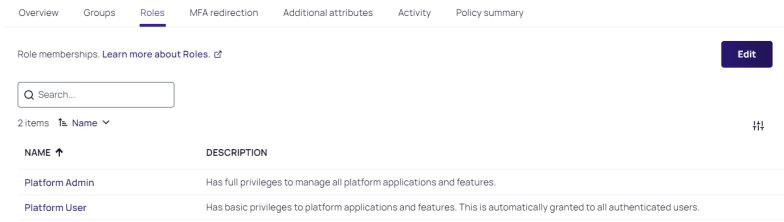


5. To remove a user from a group, hover your cursor in the group row, near the right end of the **Name** column and click the trash icon that appears.

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

Roles

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. For more detailed information about managing user roles, see "Roles and Permissions" on page 217.



MFA Redirection

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

To explain how redirection works, we've defined the following two users:

- Original login user: The user who is actively trying to log in.
- Redirect user: The user who has MFA setup. MFA will redirect to this user to answer any MFA challenges.

MFA is performed as the redirect user, on behalf of the original login user. This means any MFA mechanism that is used, such as email, text, Mobile Authenticator, etc. All are completed by the redirect user.

1. The original user attempts to login with their username.
2. The details for the original login user are retrieved from the Delinea Platform.
3. The original login 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.

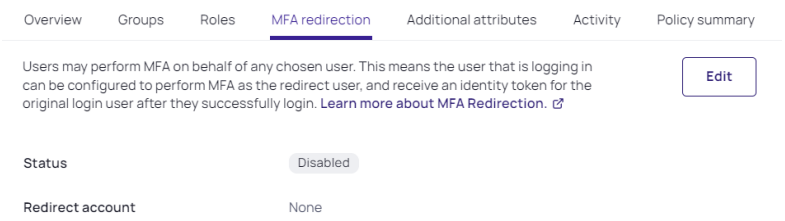
Typical MFA Redirection Use Cases

The original login user has no attributes configured, and therefore they cannot satisfy any MFA. When the original login user is challenged for additional authentication, the MFA redirection feature can be configured so the redirect

user's MFA challenges (who has the required mechanisms configured) are used for the original login user to answer.

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 box next to *Enable redirect of Multi-Factor Authentication to a different user account.*
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, you will generate an error: *Cannot redirect MFA to the same user*.

5. Click **Save**.

Additional Attributes

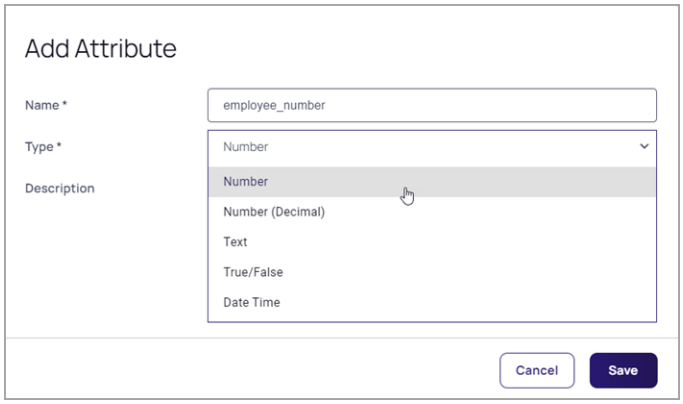
The Platform provides default user attributes, but you can add user attributes with custom values for Active Directory and Delinea Directory users. These added attributes can be useful as valid targets of MFA, for instance as an alternate email or phone number. The added attributes are stored on the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

Add User Attributes

To make attributes available for login authentication rules and SAML user authentication, you must first add them to the user table.

1. Click **Settings** from the left navigation menu, then select **User attributes**.
2. Click the **Additional attributes** tab.
3. Click **Add Attributes**.

4. Enter a name for the attribute. The name may contain only letters, numbers, and underscores. It must start with a letter, and must include at least one underscore. For example: `employee_status`.
5. Select the attribute Type from the drop-down list.

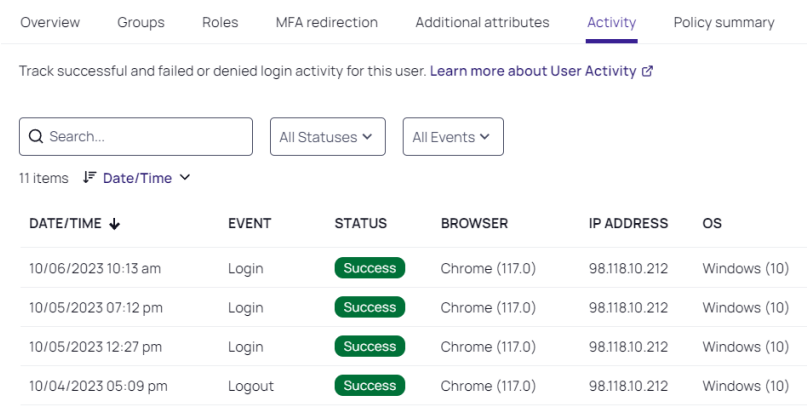


Type	Description
Number	allows whole numbers
Number (decimal)	allows numbers with decimals
Text	allows any string
True/False	results in a drop-down list for the attribute Value
Date Time	results in a date and time picker for the attribute Value

6. Enter a Description (optionally) for the attribute.
7. Click **Save**.

Activity

Click the **Activity** tab.



The Activity tab lists each of the user's activities (events) on the Platform, including the following:

- Login
- Logout
- Security Question Set
- Password Change
- Password Change Failed
- AD Password Change
- AD Password Change Failed

For each activity/event, the following information is displayed:

- Date/Time
- Event name
- Status (Success or Failed)
- Browser
- IP Address
- Operating System

Policy Summary

The **Policy Summary** tab displays all information about existing policies currently associated with a specific user, as shown in the image below. The page does not provide editing capabilities, because all of these policies are managed elsewhere.

Overview Groups Roles MFA redirection Additional attributes Activity Policy summary

Applied policy summary

Learn more about policies

Services

POLICY SETTING	VALUE	POLICY NAME
Default Profile		
Enable authentication policy controls	Yes	Default Policy
Authentication Rules	Identity cookie is not present = Default New Device Login Profile	Default Policy
Default authentication profile	Default Other Login Profile	Default Policy
Browser Session Parameters		
Allow the 'Keep me signed in' checkbox option at login (session spans browser sessions)	Yes	Default Policy
Session length (Hours)	12	Default Policy
Other Settings		
Allow users without a valid authentication factor to log in	Yes	Default Policy
Allow additional authentication from same device	Yes	

User security

POLICY SETTING	VALUE	POLICY NAME
Password Reset		
Account self service controls	Yes	Default Policy
Enable password reset	Yes	Default Policy
Password reset authentication profile	Default Password Reset Profile	Default Policy
Additional Policy Parameters		
Maximum password resets allowed during the capture window	10	Default Policy
Capture window for password resets (default 60 minutes)	60	Default Policy

Password Settings

POLICY SETTING	VALUE	POLICY NAME
Display Requirements		
Show password complexity requirements when entering a new password (default no)	Yes	Default Policy
Capture Settings		
Maximum consecutive bad password attempts allowed within window (default Off)	5	Default Policy

Devices

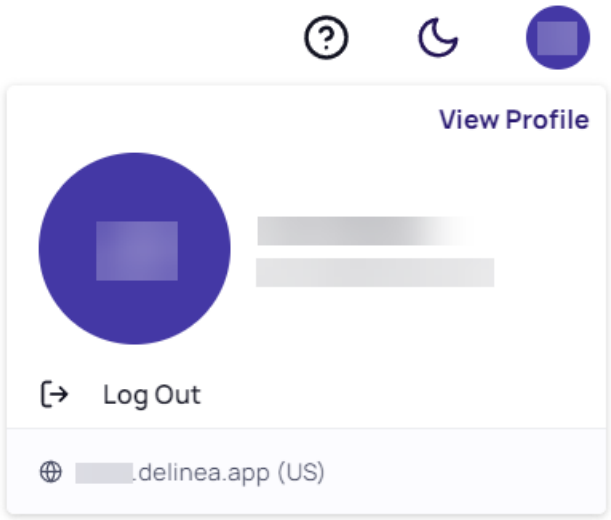
POLICY SETTING	VALUE	POLICY NAME
Permit device registration		
Enabled	Yes	Default Policy

User Profile

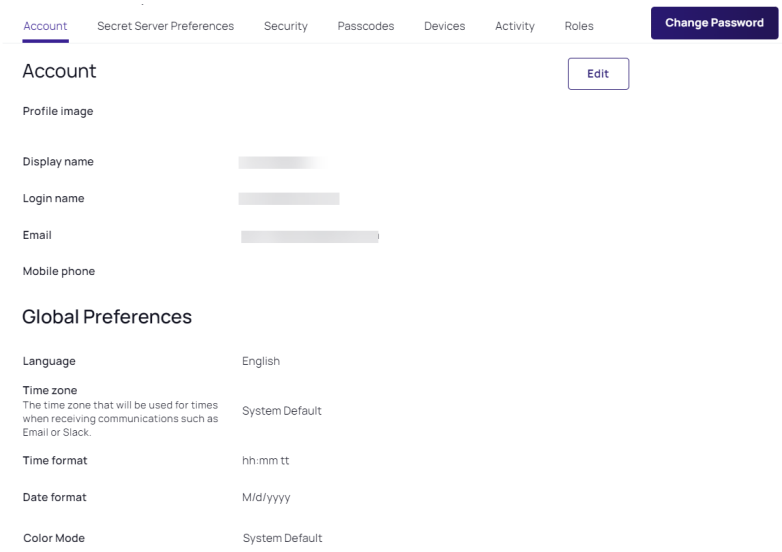
The procedure below describes how a user would view and edit their user profile settings.

1. Find your user icon at the top right of the 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.



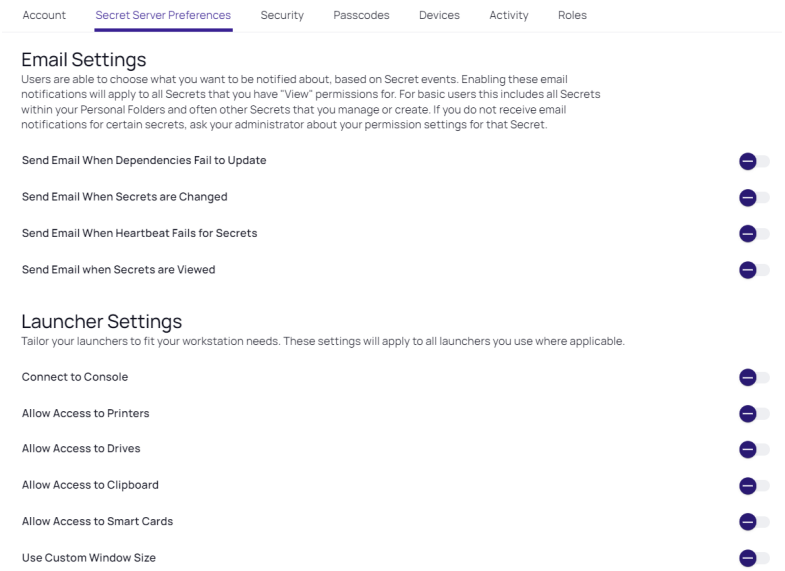
3. Click **View Profile**. Your profile page opens to the Account tab, displaying basic information about your user account and global preferences, as shown below. The page also displays a **Change Password** button in the top right corner.



4. Click the **Edit** button.
   In the Account section, you can click **Upload Image** to choose a head shot or other image for your profile, which will then be used for your user icon. The settings for Display name, Login name, Email, and Mobile phone may be editable, but if your organization controls them, they will not be editable.

   In the Global Preferences section, you can configure your preferences for date, time, and color mode.

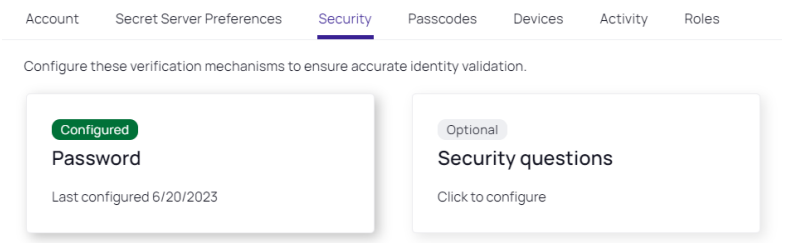
5. Click the **Secret Server Preferences** tab, where you can activate and deactivate email and launcher settings using toggle switches.



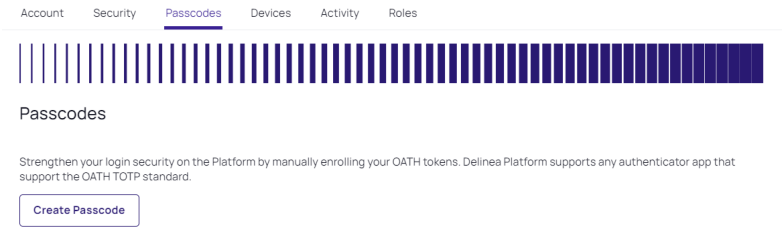
Under Email Settings, you can choose what you want to be notified about, based on Secret events. Enabling these email notifications will apply to all Secrets that you have "View" permissions for, including all secrets in your personal folders and other secrets you created or manage. If you don't receive email notifications you want to receive for a specific secret, ask your platform administrator to review your permissions for that secret.

Under Launcher Settings, you can tailor settings to fit your workstation needs for all launchers you use.

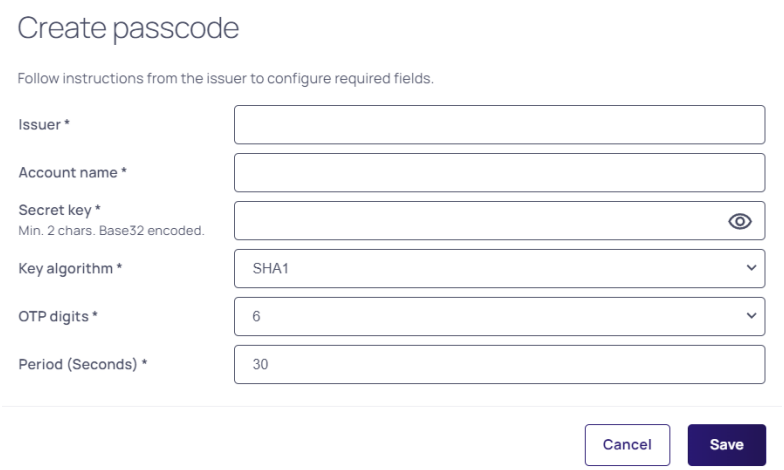
6. Click the **Security** tab. The tab displays your configured platform verification mechanisms as well as available optional mechanisms that are not yet configured. To configure an optional mechanism, click the mechanism card.



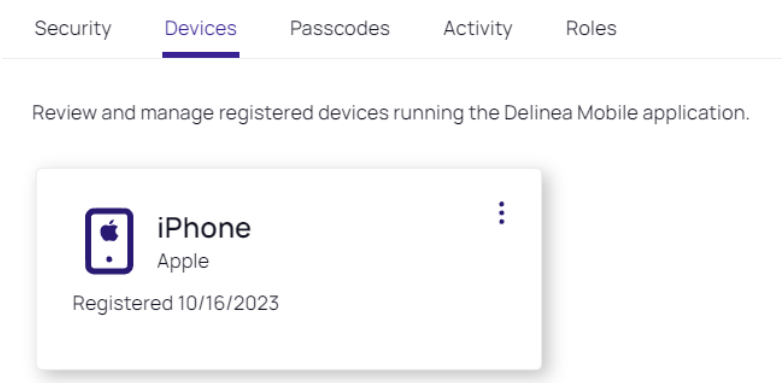
7. Click the **Passcodes** tab.



8. Click **Create Passcode** to manually enroll your OATH tokens and strengthen your platform login security. The Delinea Platform supports any authenticator application that supports the OATH TOTP standard.

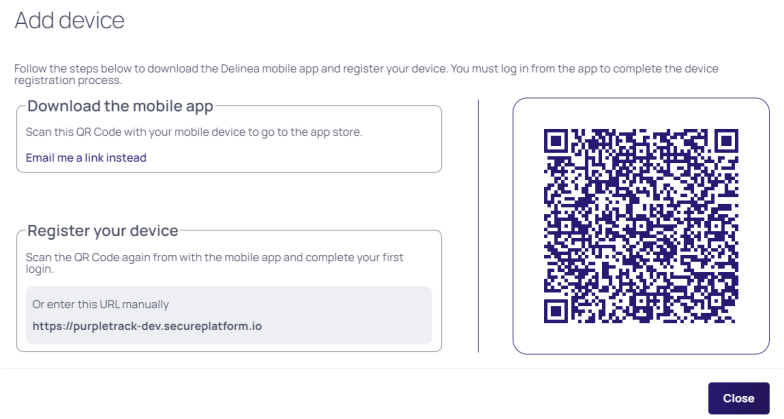


9. Complete the fields in the Create passcode dialog as follows:
   - Issuer*:
   - Account name*:
   - Secret key*:
   - Key algorithm*:
   - OTP digits*:
   - Period (Seconds)*:
10. Click **Save**.
11. Click the **Devices** tab. If you have a device registered on the platform, it appears here.

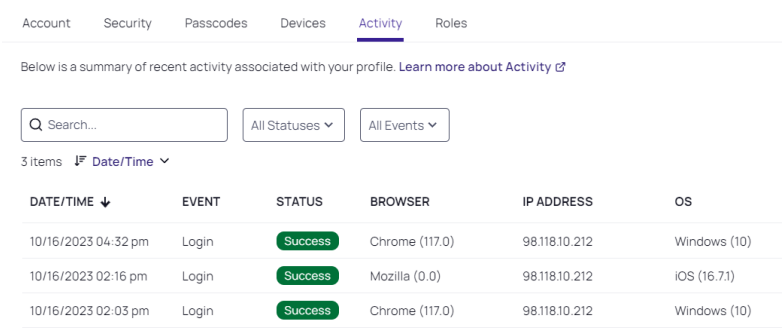


To unregister a device, click the three vertical dots on the device card and click **Unregister**.

12. To add a device, click **Add Device**.

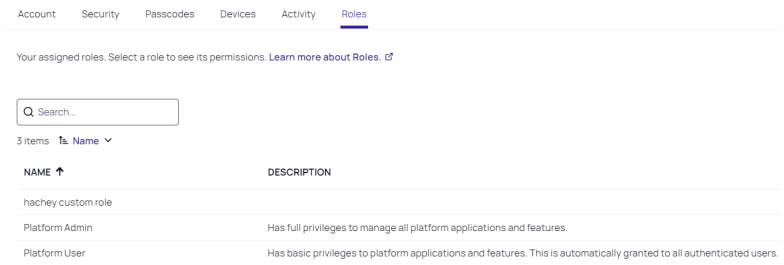


13. Follow the instructions displayed to download the Delinea Mobile application and register your mobile device.
14. Click the **Activity** tab.

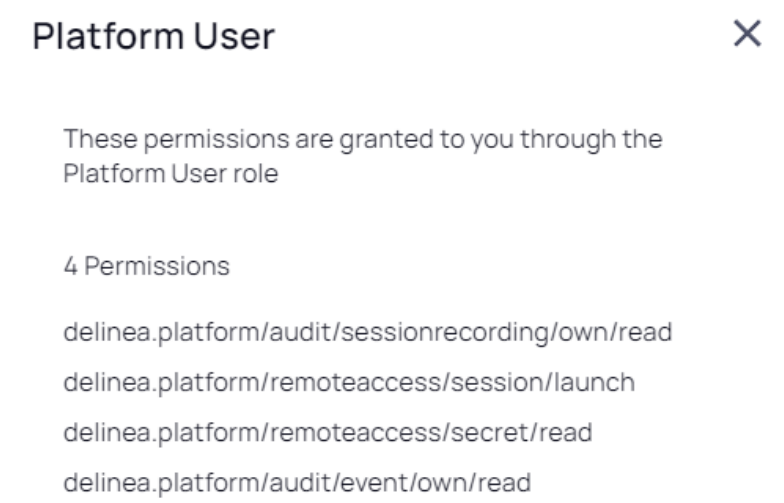


15. The activity tab displays all of your platform activities including each event and event status, the activity date and time, and the browser, IP address, and OS you used. To filter the activities displayed, use the **Search** box or the drop-down menus for **Statuses** and **Events**

16. Click the **Roles** tab. A table displays the roles you are assigned to, including the role name and description.



17. To see the permissions granted through a role, click the role name. The permissions are displayed in a panel that opens to the right.



Group Management

For new platform customers who weren't using Secret Server previously, platform groups and Secret Server groups don't need to be linked or synchronized. Platform groups are now recognized in Secret Server group interactions, without prior synchronization. For example, when a user opens a secret, clicks the **Sharing** tab, and searches for groups, Secret Server and platform groups are both queried simultaneously.

Note: If you set up a new platform group and then look immediately for the group in Secret Server, it might not appear right away. The synchronization takes place at timed intervals, and you might need to wait several minutes for the interval to arrive. To force new groups to synch immediately, follow the directions in the next section.

Manually Synchronize New Platform and Secret Server Groups

To force new groups to synch immediately:

1. Click **Settings** from the left navigation, then click **Platform groups sync**.
2. On the Platform Integration page, select the **Groups** tab.
3. Click **Edit.**
4. Click inside the box under **Select Groups**.
5. Begin typing the name of the new group and it will appear.
6. Select the box next to the group name.
7. Click **Save**.
8. Click **Sync Now**.

Note: If a new federated user does not appear on the platform, in a group or otherwise, it could be because the user has not yet logged into the platform for the first time.

Group Mappings

Group mapping is the method of associating user groups from an IdP such as Auth0 to corresponding local groups on the Delinea Platform (SP). This ensures that the user is granted the appropriate level of access based on their group memberships in the IdP's system.

Administrators can define mappings that dictate how the groups received from the IdP should be translated into specific groups on the platform.

On the Delinea Platform, federated groups are not *added* to named platform identity groups. Instead, they are *mapped* to platform groups through the IdP group's *Object ID*.

When a user logs in with an IdP's federated email domain, the platform will log them in as a federated user. The user is first authenticated when the IdP sends the platform an attribute/claim named `groups` for that user, which includes an Object ID for each IdP group that user belongs to. The Object ID maps to platform groups, and the user is added as a member of those mapped groups.

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 as described below. For more information on groups, roles, and permissions, see User Roles and Permissions.

Enabled Platform Groups

Platform permissions are unrelated to Secret Server permissions. But platform users need Secret Server permissions to access their secrets and Secret Server admin privileges. Secret Server permissions can be assigned to platform users by linking a platform group to an *Enabled Platform Group* in Secret Server, then assigning Secret Server permissions to the platform accounts in the linked Secret Server group.

Linking and Synching Groups

For platform customers who opted into the platform from an existing Secret Server implementation, platform and Secret Server groups must be linked and synchronized. When a user with administrator permissions in both the 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 identity 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 membership, so all members of Enabled Platform Groups are platform accounts. 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.

1. Click **Settings** from the left navigation, then click **Platform groups sync**.
2. On the Platform Integration page, select the **Groups** tab.
3. Next to Enabled Platform Groups, click **Edit**.
4. In the **Select Groups** box, enter the name of a platform group you wish to synch to a Secret Server group. Secret Server immediately begins to query the platform identity service and when it finds the group you're searching for, the group's name is displayed beneath the Search field with a check box next to it.
5. Select the box next to group's displayed name.
6. Click **Save**.
7. Click **Sync Now**.

After the platform and Secret Server groups are linked and synchronized, you can find the new Secret Server group from anywhere in Secret Server where groups are referenced. When you click to open the synched group, the group's page opens with a banner at the top stating, *The members of this group are managed by Platform*.

Assigning Secret Server Permissions to Platform Users

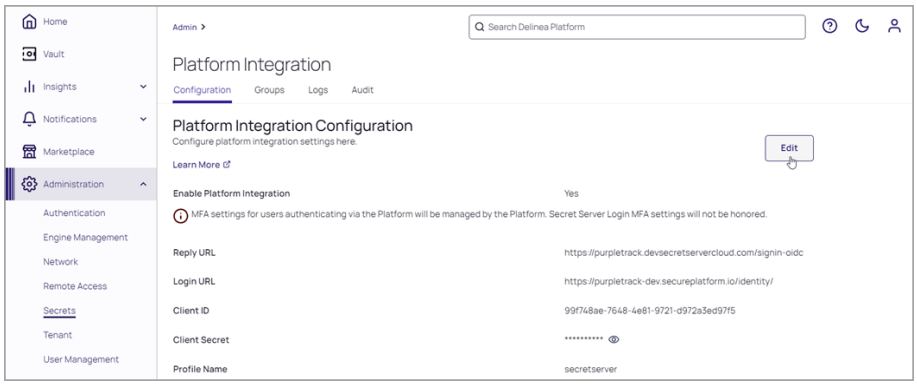
Platform permissions are unrelated to Secret Server permissions. But platform users need Secret Server permissions to access their secrets and Secret Server admin privileges. Secret Server permissions can be assigned to platform users by linking a platform to an Enabled Platform Group in Secret Server, then assigning Secret Server permissions to the platform accounts in the linked Secret Server group.

1. Click **Access** from the left navigation menu, then select **Groups**.
2. Click to open an Enabled Platform Group.
3. Click the **Roles** tab.
4. Next to **Group Roles**, click **Edit**. A list opens of all available Secret Server roles (with attached permissions).
5. Check the box next to each role you wish to assign to the group.
6. Click **Save**.

Automatically Create Groups During Synchronization

Instead of manually linking a Secret Server group to a platform group, you can choose to automatically create new Enabled Platform Groups in Secret Server during the periodic group synchs. When you enable the Create Groups During Synchronization feature, Secret Server checks all associated platform users to see if any belong to a platform group that is not yet linked to a Secret Server group. If an unlinked platform group is found, Secret Server automatically creates and links a corresponding Secret Server group.

1. Click **Settings** from the left navigation menu.
2. On the Settings page, click **Platform integration**. The Platform Integration page opens to the Configuration tab.



3. Click **Edit** next to Platform Integration Configuration.
4. Scroll down and select the box next to **Create Groups During Synchronization**.
5. Consider the warning message that appears:
   Warning! Enabling "Create Groups During Synchronization" can create a large number of groups locally if the Platform users are members of many groups in Platform, including groups through external directory services such as Active Directory or Microsoft Entra ID federation.
6. Click **Cancel** to cancel, or click **Save** to automate the creation of new Enabled Platform Groups in Secret Server during the periodic group synchs.

Predefined Groups

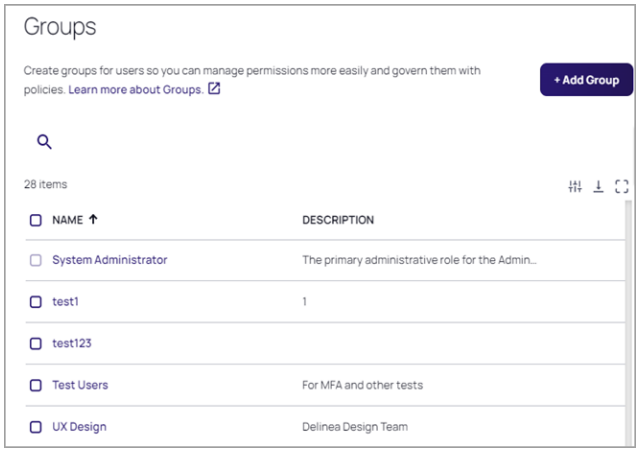
The Delinea Platform has two predefined groups:

- **Everybody**: All platform users belong to the Everybody group, and through that group membership they inherit the Platform User role, with permissions to log in to platform, access their secrets, launch RAS 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. At tenant creation, the user account that is created automatically belongs to the System Administrator group. The System Administrator group cannot be renamed or deleted.

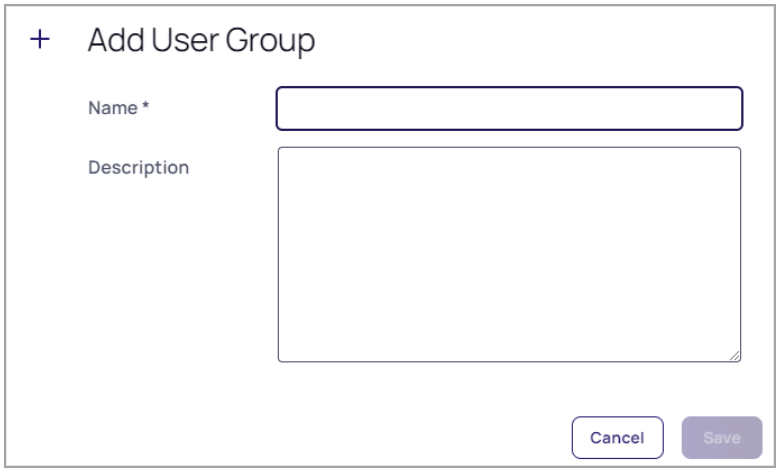
For more information on groups, roles, and permissions, see "Roles and Permissions" on page 217.

Adding a Group

1. Click **Access** from the left navigation, then select **Groups**.



2. To add a group, click the **Add Group** button.

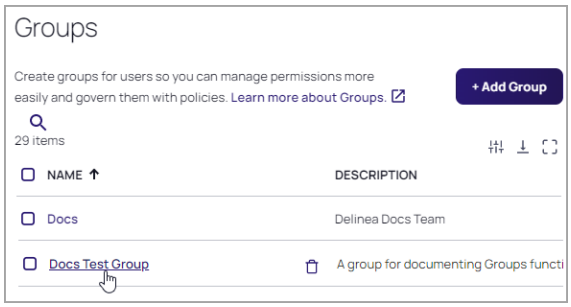


3. Click **Save**.
4. On the **Add group** page, enter a group **Name** and **Description**
5. Click **Save**.

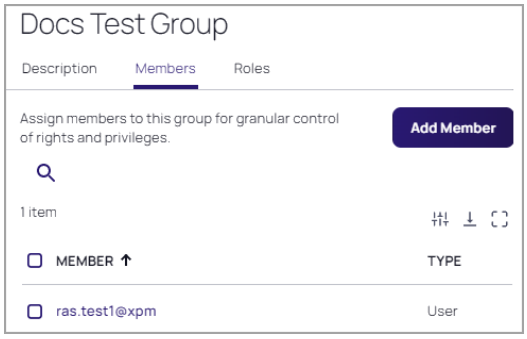
Adding Users to a Group

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:

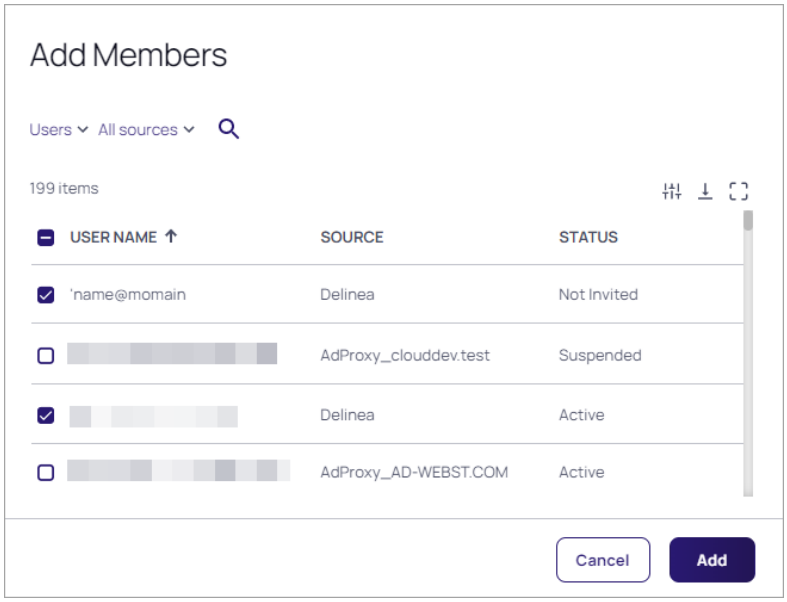
1. Click **Access** from the left navigation menu, then select **Groups**.
2. On the **Groups** page, click a group.



3. On the specific group's page, click the **Members** tab.



4. Click the **Add Member** button.
5. On the **Add Members** page, Check the box next to each user you want to add, then click the **Add** button.

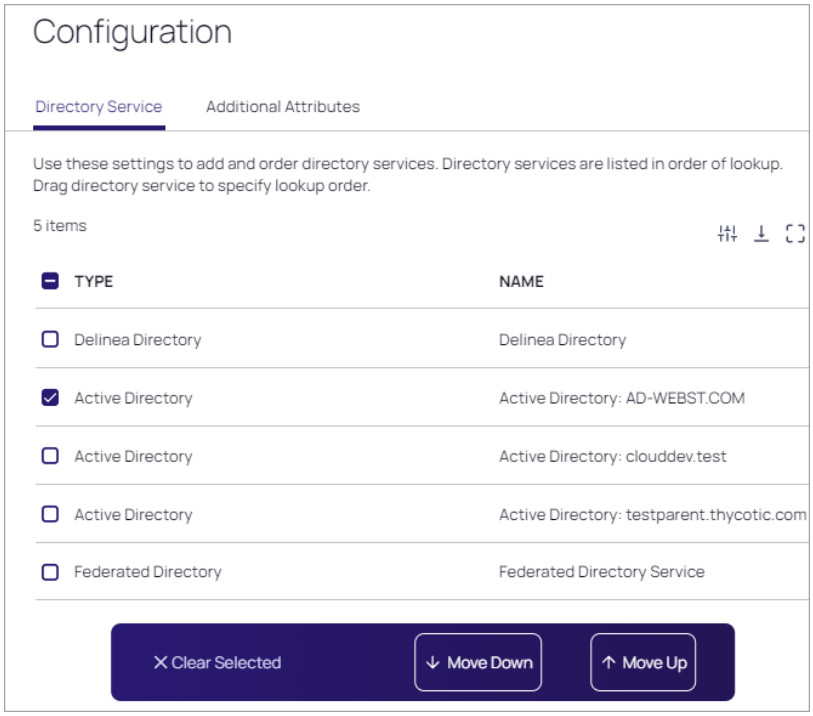


A pop-up notice appears, saying, **Member has been Added Successfully**. A pop-up notice appears, saying, **Member has been Added Successfully**.

User Directory Service Configuration

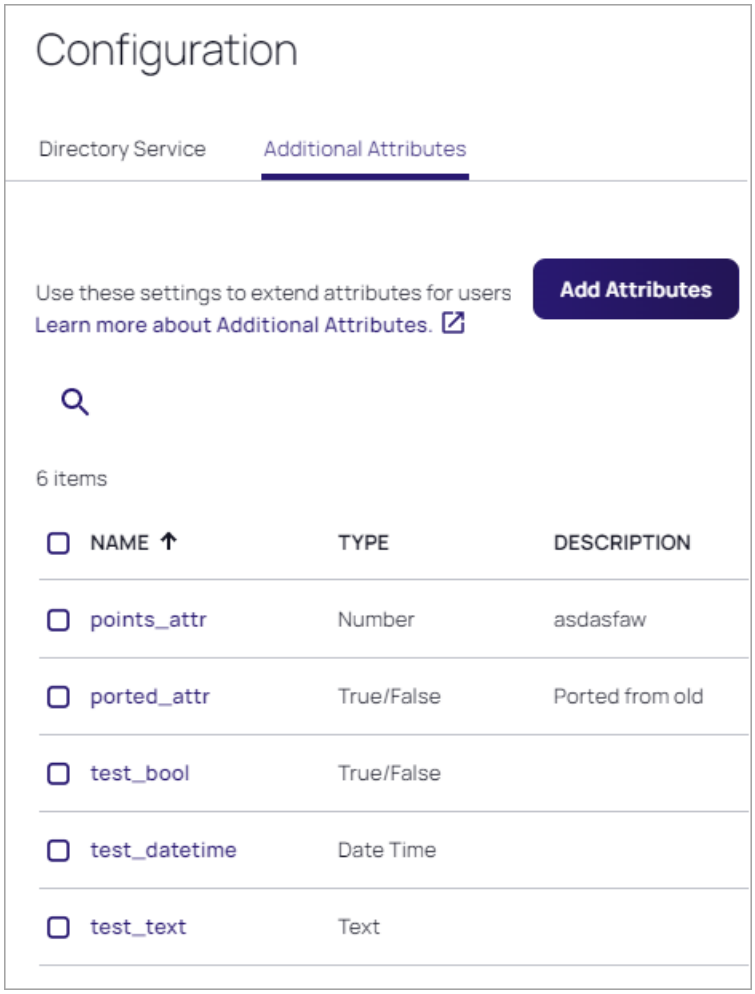
1. Click **Settings** from the left navigation, then select **Directory services**. Delinea Directory will always be at the top of the list, and Federated Directory will always be at the bottom.
2. Check the box next to a directory service you want to use or remove. Actions available for a selected directory 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 pop-up appears with options that could include one or more of the following, depending on the type of directory or directories you've selected: **Clear Selected**, **Move Down**, **Move Up**, or **Remove Selected**

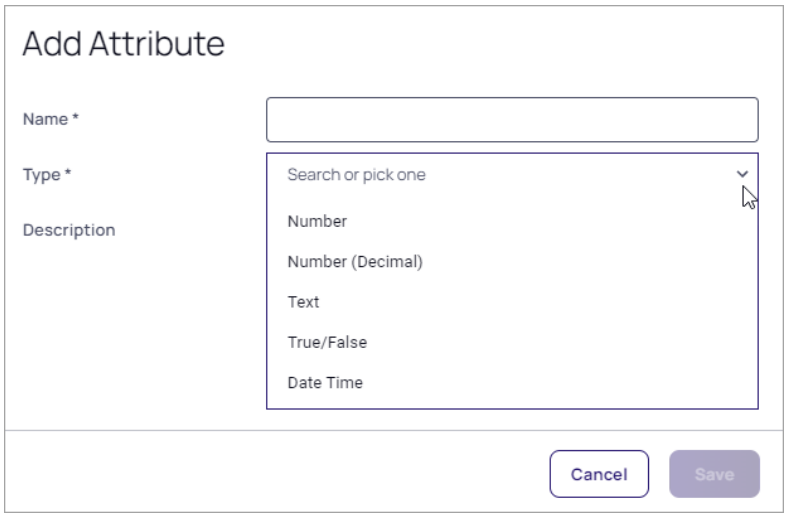


Additional Attributes

1. On the Configuration page, click the **Additional Attributes** tab.



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. The name can contain only letters, numbers, and underscores. It must begin with a letter and contain at least one underscore.



4. In the **Type** field, search for a type or click the drop-down arrow to pick one of the following:
   - Number
   - Number (Decimal)
   - Text
   - True/False
   - Data Time
5. Click **Save**. A pop-up notice appears, saying, **Your Attribute has been Added Successfully**.

Roles and Permissions

The Delinea Platform's role-based access control system precisely manages resource access, allowing you to authorize users with the exact permissions they need.

Unified Roles and Permissions in Secret Server and Platform

For new customers of the Delinea Platform and Secret Server, all roles and permissions are now centrally managed within the Platform.

As of November 8, 2023, all newly provisioned customers on the Delinea Platform will experience a unified roles and permissions system. All Secret Server roles and permissions are now managed centrally within the Platform.

- The 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 removeable, however the Platform User role provides basic permissions for a user to log into platform, launch RAS 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, and those topics are covered below.

Permissions

Platform permissions are made available for assignment to Roles according to the services available in your platform environment.

Users, Groups, Roles, and Permissions

To understand the relationships between users, groups, roles, and permissions, review the following points:

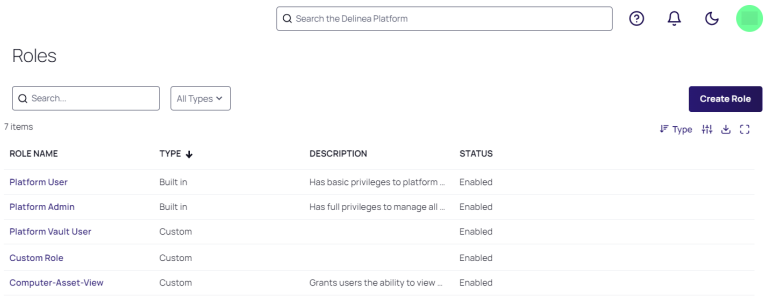
- A permission can be assigned to one or more roles, but cannot be assigned directly to a group or a user.
- A role can be assigned to one or more groups, and a group can be assigned to one or more users.
- A user inherits one or more roles, along with each role's permissions, through the group or groups the user is assigned to.

Note: Although the platform currently 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.

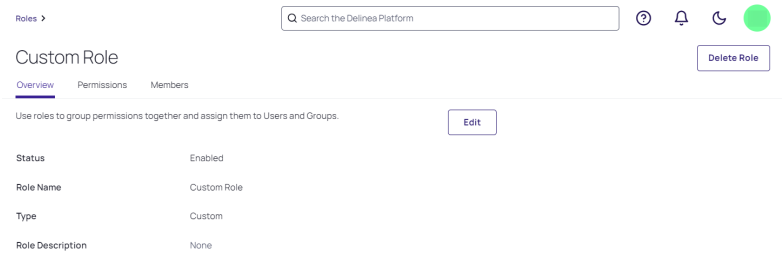
Edit Role Permissions

To edit an existing role, follow the steps below.

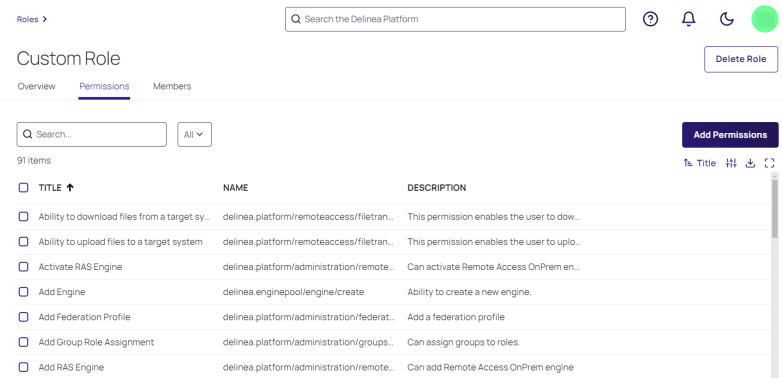
1. Click **Access** from the left navigation menu, then select **Roles**.



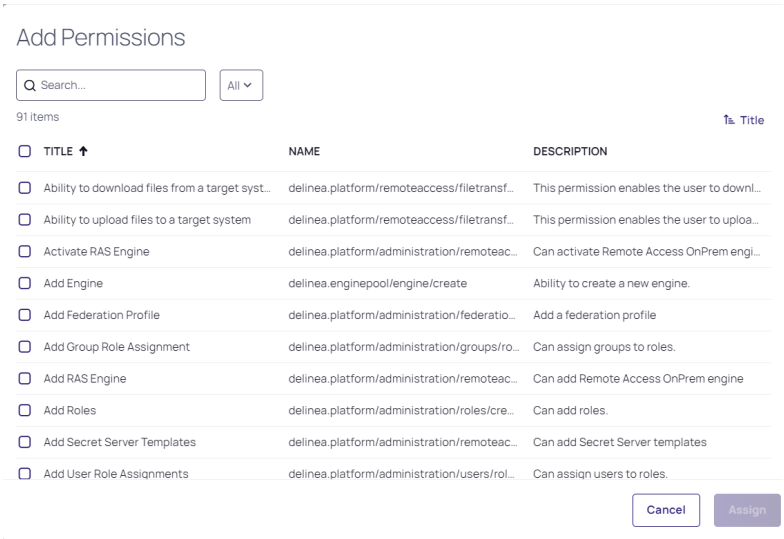
2. Click the name of one of the roles displayed. The role page opens to the Overview tab.



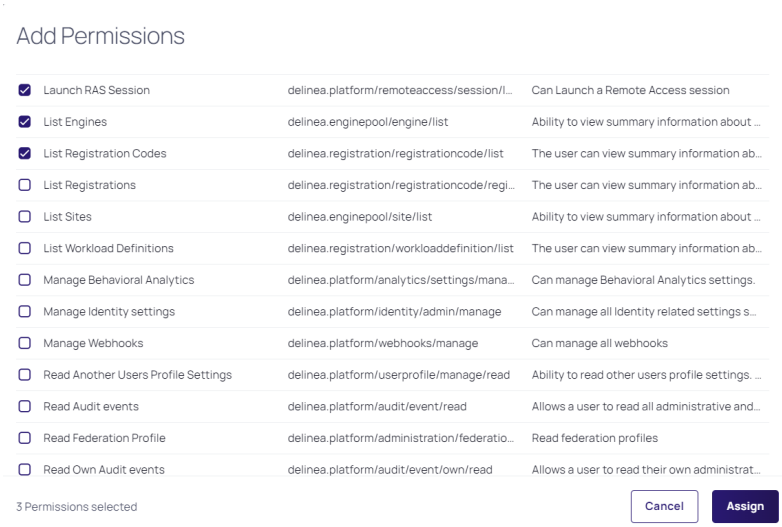
3. Click the **Permissions** tab. All permissions assigned to the role are listed on the tab.



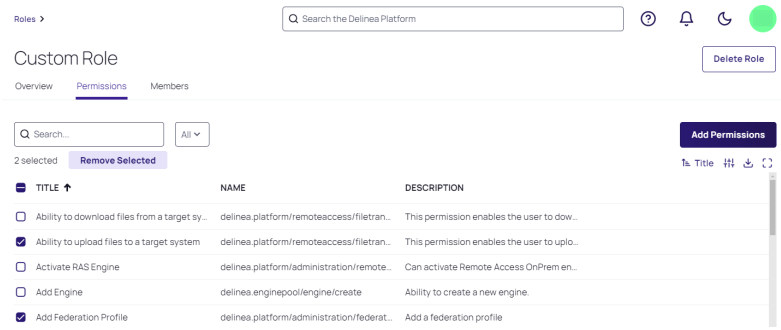
4. To add a permission to the role, click **Add Permission**. The Add Permissions dialog pops up.



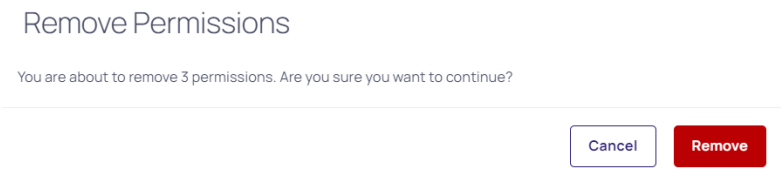
5. Select the box next to each permission you would like to add to the role.



6. Click **Assign**.
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**.

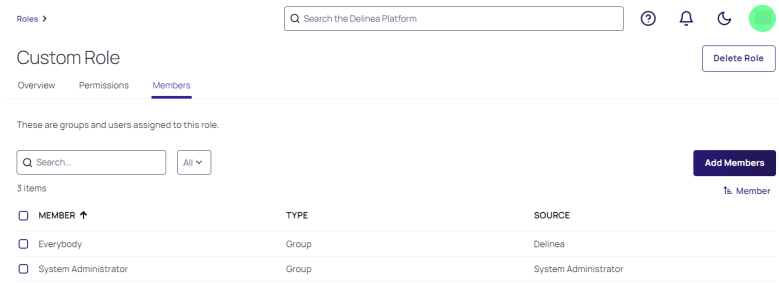


8. Click **Remove** from the pop-up banner to confirm that you want to remove the permission(s).

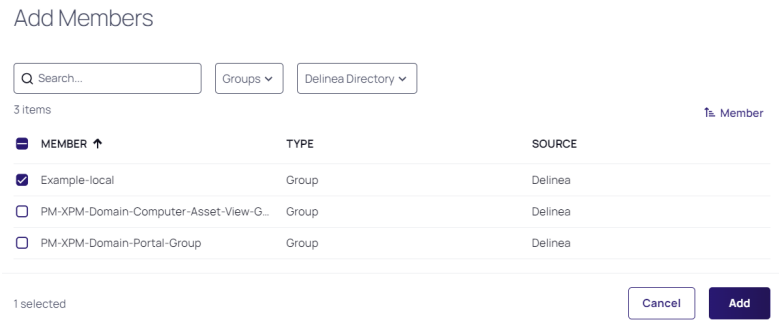


Edit Role Members (Groups)

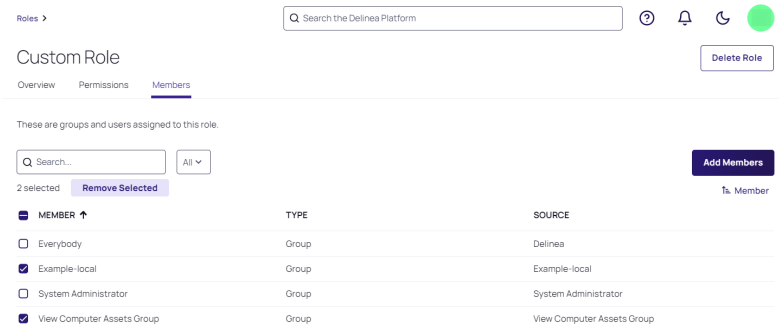
1. Click the **Members** tab.
2. To add members (groups) to the role, click **Add Members**.



3. The Add Members dialog pops up.

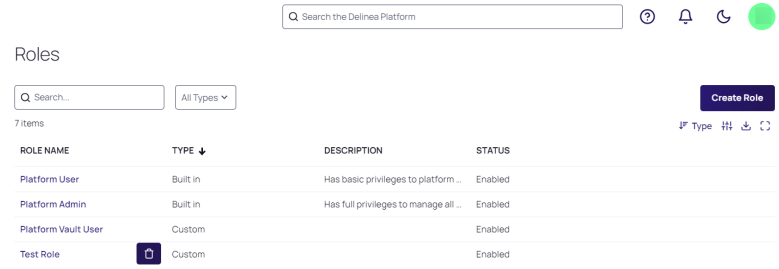


4. Select the box next to the groups you want to add, then click **Add**.
5. To remove members (groups) from the role, go to the Members tab and select the box next to each group you wish to delete, then click **Remove Selected.**

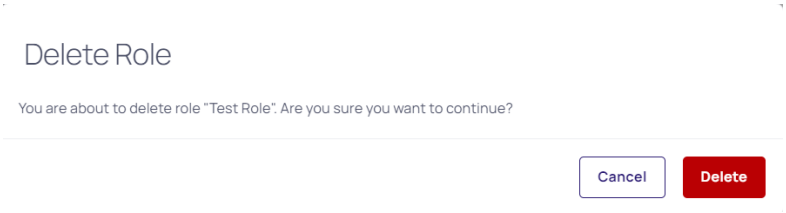


Delete a Role

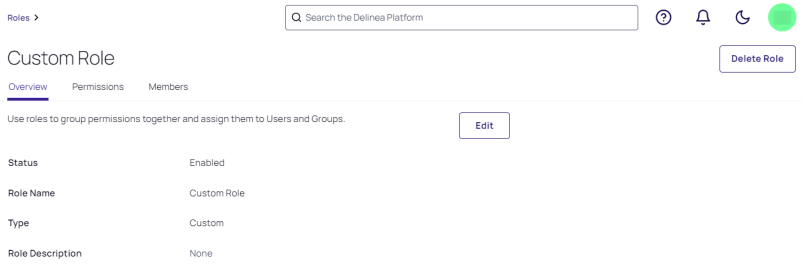
1. Click **Access** from the left navigation menu, then select **Roles**.
2. Hover your cursor over the role you wish to delete, then click the trash icon that appears.



3. Click **Delete** from the confirmation pop-up.

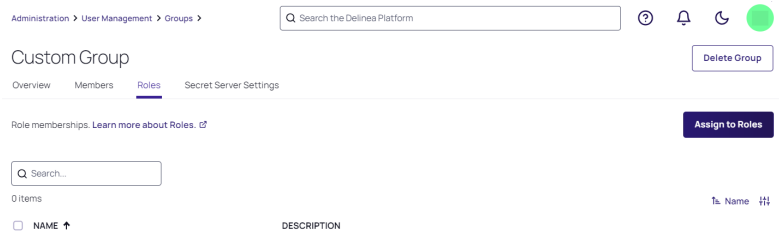


Note: You can also delete a role directly from the role's details page by clicking the **Delete** button at the top right of the page.

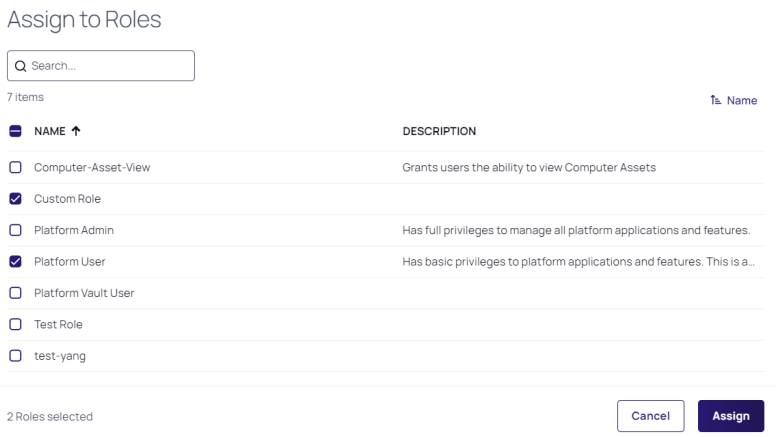


Assign a Group to a Role

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**.

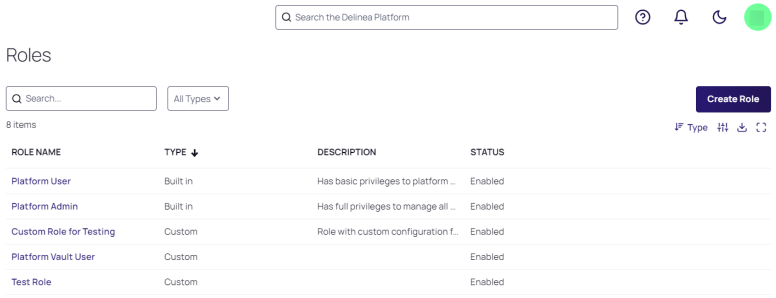


4. Select the role(s) and click **Assign**.

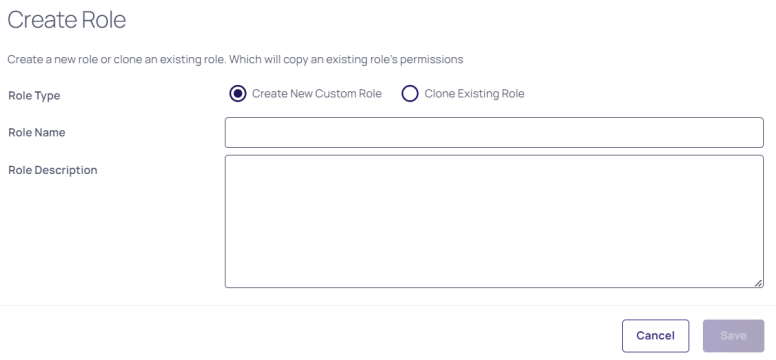


Create a New Role

1. Click **Access** from the left navigation menu, then select **Roles**.

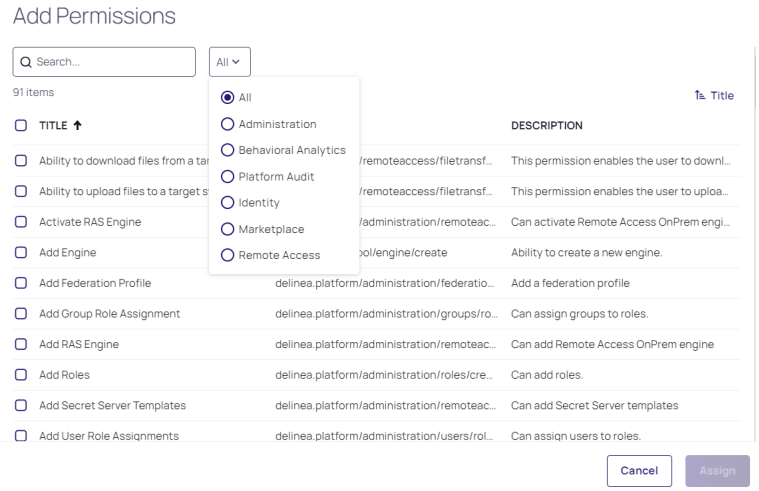


2. Click **Create Role**.
3. To create a new role from scratch, select **Create New Custom Role**. To create a role by cloning an existing role and editing it, select **Clone Existing Role**.



4. Enter appropriate information in the **Role Name** and **Role Description** fields.
5. Click **Save**.

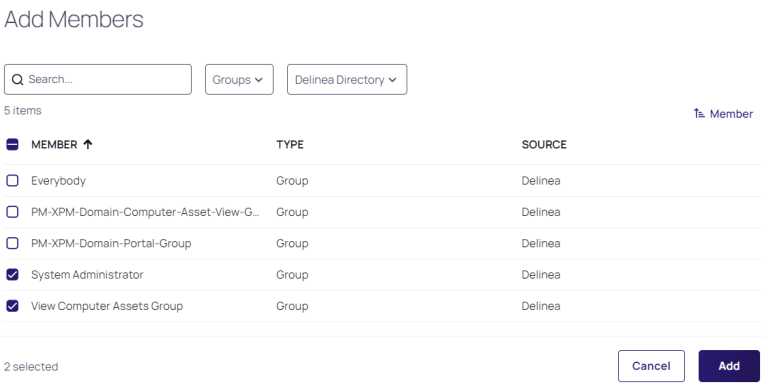
6. Click the **Permissions** tab.
7. Click **Add Permissions** to assign appropriate permissions to the role.
   - To search through existing permissions, enter terms into the Search box.
   - To restrict your search results to just one type of permission, make your selection from the **All** drop-down.



8. Click **Assign**.

Add Members (Groups) to a Role

1. Click the **Members** tab.
2. Click **Add Members**.



   - To Search through existing groups, enter terms into the Search box.
   - The first search filter is set to restrict search results to **Groups** by default. Although you can select Users from the drop-down, adding individual users to a role is not considered a best practice.

- To search across a specific directory (for example Active Directory), click the Delinea Directory drop-down and select the desired directory.

3. When you have made your selections, click **Add**.

Platform 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
Activate RAS Engine	Activate Remote Access OnPrem engine	delinea.platform/administration/remoteaccess/engine/activate
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 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 RAS Engine	Add Remote Access OnPrem engine	delinea.platform/administration/remoteaccess/engine/create
Add Roles	Add roles	delinea.platform/administration/roles/create
Add Secret	Create new Secrets. The Add permission no longer includes the role permission, View Secret.	delinea.vault/secretserver/secret/create

Permission Name	Description	Permission String
Add Secret Server Templates	Add Secret Server templates	delinea.platform/administration/remoteaccess/secrettemplate/create
Add User Role Assignments	Assign users to roles	delinea.platform/administration/users/roleassignment/create
Administer Analytics	View and edit the settings for analytics.	delinea.analytics/settings/administer
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 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

Permission Name	Description	Permission String
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 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
Administer Discovery	View and import computers and accounts that are found by Discovery.	delinea.discovery/discovery/administer
Administer Distributed Engine Configuration	Update the Distributed Engine configuration.	delinea.vault/secretserver/administration/distributedengine/administer

Permission Name	Description	Permission String
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 Groups	View, edit, create, and disable groups. Also allows users to assign users to groups and remove users from groups.	delinea.directory/administration/groups/administer
Administer HSM Configuration	Change configuration or disable the use of a Hardware Security Module (HSM).	delinea.vault/secretserver/administration/hsm/administer
Administer Inbox	Administer notification settings for the inbox.	delinea.inbox/inbox/administer

Permission Name	Description	Permission String
Administer IP Addresses	Create, edit, and delete IP Address Ranges. These ranges are used to restrict certain users to specific IP Addresses.	delinea.directory/ipaddresses/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 Licenses	View, edit, install, and delete licenses.	delinea.license/administration/licenses/administer
Administer Platform Integration	Manage the Secret Server connection to the Delinea platform.	delinea.vault/secretserver/administration/platformintegration/administer
Administer Radius Server Configuration	Manage radius client settings	delinea.platform/identity/radius/administer
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

Permission Name	Description	Permission String
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	Allows a user to 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

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

Permission Name	Description	Permission String
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 Session Recording Configuration	View and edit session recording settings on the Session Recording tab of Configuration settings.	delinea.audit/administration/sessionrecording/manage
Administer session recordings	View and terminate active launcher sessions.	delinea.audit/administration/sessionrecording/manage
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 Users	Create, disable, and edit users in the system.	delinea.directory/administration/users/administer
Administer Workflows	Manage workflows (advanced access management).	delinea.vault/secretserver/administration/workflows/administer

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/listsecretaccess forassigningpolicy/allow
Approve Registratio n	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
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

Permission Name	Description	Permission String
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 via 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
Configure Secret Server integration	Configure Secret Server integration	delinea.platform/administration/remoteaccess/vault/configure
Copy Secret	Copy secrets when the user also has Own Secret role permission.	delinea.vault/secretserver/secret/copy

Permission Name	Description	Permission String
Create a Site	Create a new site.	delinea.enginepool/site/create
Create Engine	Create a new engine.	delinea.enginepool/engine/create
Create Engine Pool Group	Create a new engine pool group.	delinea.enginepool/group/create
Create Policy	Create Policies	delinea.policy/policies/create
Create RAS Site	Create a new Remote Access site to install engines	delinea.platform/administration/remoteaccess/site/create
Create Registration Code	Create a Registration Code	delinea.registration/registrationcode/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
Create Users	Create new local users in Secret Server, but not edit them once created.	delinea.directory/administration/users/create
Deactivate Secret	Mark secrets as deactivated.	delinea.vault/secretserver/secret/deactivate
Deactive a Secret within a Report	Run the delete Secrets action from a report.	delinea.vault/secretserver/administration/reports/secretfromreport/deactivate
Delete a Site	Delete a site.	delinea.enginepool/site/delete

Permission Name	Description	Permission String
Delete Engine	Delete an engine.	delinea.enginepool/engine/delete
Delete Engine Pool Group	Delete an engine pool group.	delinea.enginepool/group/delete
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 Policy	Delete Policies	delinea.policy/policies/delete
Delete RAS Engine	Delete Remote Access OnPrem engine	delinea.platform/administration/remoteaccess/engine/delete
Delete RAS Site	Delete Remote Access site	delinea.platform/administration/remoteaccess/site/delete
Delete Roles	Delete roles.	delinea.platform/administration/roles/delete
Delete Secret Server Templates	Delete Secret Server templates	delinea.platform/administration/remoteaccess/secrettemplate/delete
Delete User Role Assignment	Remove users from roles.	delinea.platform/administration/users/roleassignment/delete
Download applications and integrations	Download applications and integrations	delinea.platform/marketplace/plugins/download

Permission Name	Description	Permission String
Download Auto Export	View all automatic export tabs and download exports from cloud storage (cloud customers only)	delinea.vault/secretserver/administration/autoexport/download
Edit Policy	Edit Policies	delinea.policy/policies/update
Edit Secret	Edit a secret. If disabled, a user cannot edit secrets regardless of the secret permission.	delinea.vault/secretserver/secret/update
Enable Policy	Enable Policies	delinea.policy/policies/enable
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. Note that you can assign Administer Unlimited Admin Configuration to one user and Unlimited Administrator to another user. This would require one user to turn on the mode and another user to view and edit secrets. Formerly Administer Unlimited Admin Configuration.	delinea.vault/secretserver/administration/unlimitedadmin/administer

Permission Name	Description	Permission String
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
Generate a Device Code	Generate a Device Code	delinea.registration/devicecode/generate
Launch RAS Session	Launch a Remote Access session	delinea.platform/remoteaccess/session/launch
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
List Engine Pool Groups	View summary information about all engine pool groups.	delinea.enginepool/group/list
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

Permission Name	Description	Permission String
List Registrations	View summary information about all registrations for a registration-code	delinea.registration/registrationcode/registration/list
List Sites	View summary information about all sites.	delinea.enginepool/site/list
List Workload Definitions	View summary information about all workload-definitions	delinea.registration/workloaddefinition/list
Manage Identity settings	Manage all Identity related settings such as users, groups, policies and more	delinea.platform/identity/admin/manage
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
Publish Audit event	Create and publish audit event	delinea.platform/audit/event/create
Read Audit event	Read audit events	delinea.platform/audit/event/read
Read Federation Profile	Read federation profiles	delinea.platform/administration/federation/profile/read

Permission Name	Description	Permission String
Read Own Audit events	Read own audit events	delinea.platform/audit/event/own/read
Register a Workload	Register a Workload with a Registration Code	delinea.registration/registrationcode/register
Retrieve a Registration	Read detailed information (including sensitive information) about individual registrations	delinea.registration/registration/read
Retrieve Engine	Read detailed information about an engine.	delinea.enginepool/engine/read
Retrieve Engine Pool Group	Read detailed information about an engine pool group.	delinea.enginepool/group/read
Retrieve Registration Code	Read detailed information (including sensitive information) about individual registration-codes	delinea.registration/registrationcode/read
Retrieve Site	Read detailed information about a site.	delinea.enginepool/site/read
Retrieve Workload Definition	Read detailed information (including sensitive information) about individual workload-definitions	delinea.registration/workloaddefinition/read
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

Permission Name	Description	Permission String
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
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. Note that another user with the Administer Unlimited Admin Configuration role permission would still need to turn this mode on.	delinea.vault/secretserver/administration/unlimitedadmin/unlimitedadministrator

Permission Name	Description	Permission String
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
Update a Site	Edit a site	delinea.enginepool/site/update
Update All Session Recordings	Comment and tag session recordings	delinea.platform/audit/sessionrecording/admin/update
Update Audit event	Update audit event	delinea.platform/audit/event/update
Update Audit Setting	Update audit setting	delinea.platform/administration/audit/update
Update Engine	Edit an engine.	delinea.enginepool/engine/update
Update Engine Pool Group	Edit an engine pool group.	delinea.enginepool/group/update
Update Federation Profile	Update a federation profile	delinea.platform/administration/federation/profile/update
Update RAS Engine	Upgrade Remote Access OnPrem engine	delinea.platform/administration/remoteaccess/engine/update
Update RAS Site	Update Remote Access site	delinea.platform/administration/remoteaccess/site/update

Permission Name	Description	Permission String
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
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 All Session Recordings	View all session recordings	delinea.platform/audit/sessionrecording/admin/read
View Analytics	View, but not edit, settings for analytics.	delinea.analytics/settings/read

Permission Name	Description	Permission String
View Audit Data Retention	View retained audit data. This permission does not automatically come with the Administrator role.	delinea.insights/administration/dataretention/read
View Audit Settings	View audit settings	delinea.platform/administration/audit/read
View Auto Export	View all automatic export tabs.	delinea.vault/secretserver/administration/autoexport/read
View Computers	View computer assets	delinea.assets/computer/view
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
View Discovery	View, but not edit, computers and accounts that are found by Discovery.	delinea.discovery/discovery/read
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

Permission Name	Description	Permission String
View Dual Control Settings	View configured Dual Control settings for reports and Secret sessions.	delinea.vault/secretserver/administration/dualcontrol/read
View Enterpise 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 Group Role Assignment	View roles assigned to groups.	delinea.platform/administration/groups/roleassignment/read
View Groups	See which groups exist in the system, and which users belong to each group.	delinea.directory/administration/groups/read
View HSM Configuration	View the Hardware Security Module (HSM) configuration settings.	delinea.vault/secretserver/administration/hsm/read
View Identity settings	View Identity related settings such as users, groups, policies, and more	delinea.platform/identity/admin/read
View Inactive Secrets	View Secrets that have been deleted in the system.	delinea.vault/secretserver/secret/inactivesecrets/read

Permission Name	Description	Permission String
View IP Addresses	View IP Address Ranges that have been created to restrict access. Does not allow a user to edit these ranges.	delinea.directory/ipaddresses/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
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 Licenses	View, but not edit, the licenses in the system.	delinea.license/administration/licenses/read
View Marketplace	View the marketplace	delinea.platform/marketplace/plugins/view
View OpenID Connect	View OpenID Connect integration settings in the Configuration Login tab	delinea.platform/administration/federation/profile/read

Permission Name	Description	Permission String
View Other User/Group Permissions	Read the permissions of other users and groups.	delinea.platform/administration/haspermission/read
View Own Session Recordings	Open and view their personal session recordings	delinea.platform/audit/sessionrecording/own/read
View permissions	View permissions.	delinea.platform/administration/permissions/read
View Platform Groups	View Platform Groups	delinea.platform/administration/groups/read
View Platform Integration	View the Secret Server connection to the Delinea platform.	delinea.vault/secretserver/administration/platformintegration/read
View Platform Users	View Platform Users	delinea.platform/administration/users/read
View Policy	View Policies	delinea.policy/policies/read
View Radius Server Configuration	View radius client settings	delinea.platform/identity/radius/read
View RAS Engine	View Remote Access OnPrem engine	delinea.platform/administration/remoteaccess/engine/read
View RAS Site	View Remote Access Site	delinea.platform/administration/remoteaccess/site/read

Permission Name	Description	Permission String
View Remote Password Changing Settings	View, but not edit, Heartbeat and Remote Password Changing settings	delinea.vault/secretserver/administration/remotepasswordchanging/read
View Roles	View roles.	delinea.platform/administration/roles/read
View Secret	View secret. If disabled 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 will only be able to view 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
View Secret Server Folders	View, but not edit, folders in the system.	delinea.vault/secretserver/administration/folders/read

Permission Name	Description	Permission String
View Secret Server integration	View Secret Server integration	delinea.platform/administration/remoteaccess/vault/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. See Browse 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

Permission Name	Description	Permission String
View Secret Server Security Hardening Report	View the Security Hardening Report.	delinea.vault/secretserver/administration/securityhardeningreport/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
View Secret Server Templates	View, but not edit, Secret Templates.	delinea.vault/secretserver/administration/secrettemplate/read
View Secret Server Templates	View Secret Server templates	delinea.platform/administration/remoteaccess/secrettemplate/read
View Secret Session Recording	View recorded sessions within Secret Server.	delinea.vault/secretserver/administration/sessionrecording/read
View Secrets	View Secrets to launch RAS Session	delinea.platform/remoteaccess/secret/read

Permission Name	Description	Permission String
View Session Recording Configuration	View session recording settings on the Session Recording tab of Configuration settings.	delinea.audit/administration/sessionrecording/read
View session recordings	View active launcher sessions.	delinea.audit/sessionrecording/readall
View Session Recordings UI	Can view the Insights → Audit → Session Recordings UI	delinea.platform/audit/sessionrecording/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 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 Tenant Profile	See "Tenant" under the Administration section as well as view any/ all information on the Tenant Profile page. However, you will not be able to update that information.	delinea.platform/administration/tenantprofile/read

Permission Name	Description	Permission String
View User Audit Report	View, but not edit, the User Audit Report.	delinea.vault/secretserver/administration/useraudit/report/read
View User Role Assignments	View roles assigned to users.	delinea.platform/administration/users/roleassignment/read
View Users	View which users exist in the system.	delinea.directory/administration/users/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

Delinea Engine Management

The Delinea Platform manages and protects endpoints using small software packages called engines.

Engine Management Components

The components of the Engine Management service are as follows:

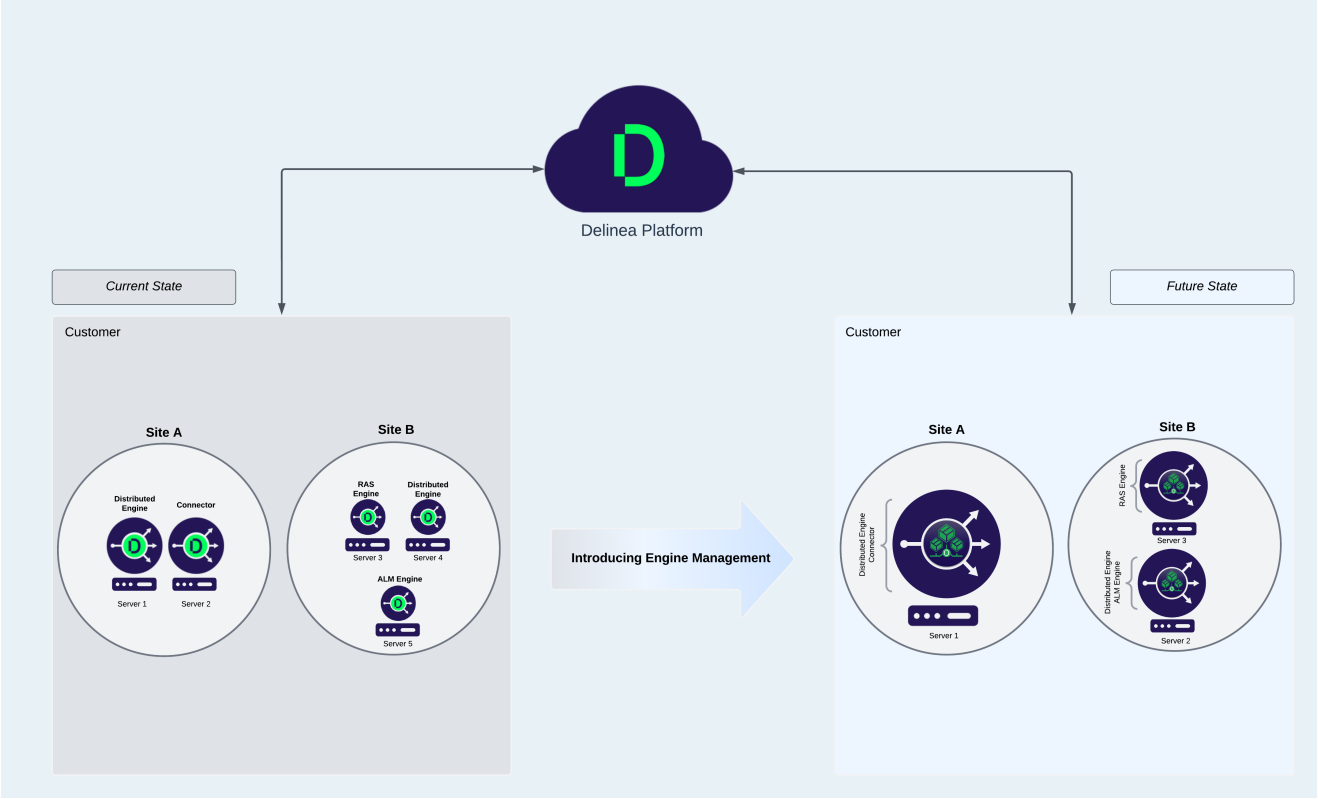
Component	Description
Site	A group of engines selected on a common principle, e.g. network or subnet, or geographical location (office, city, etc.), or data center, or any other characteristics that the IT personnel finds appropriate. Workload settings are organized at the site level.
Engine	A system agent or 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.

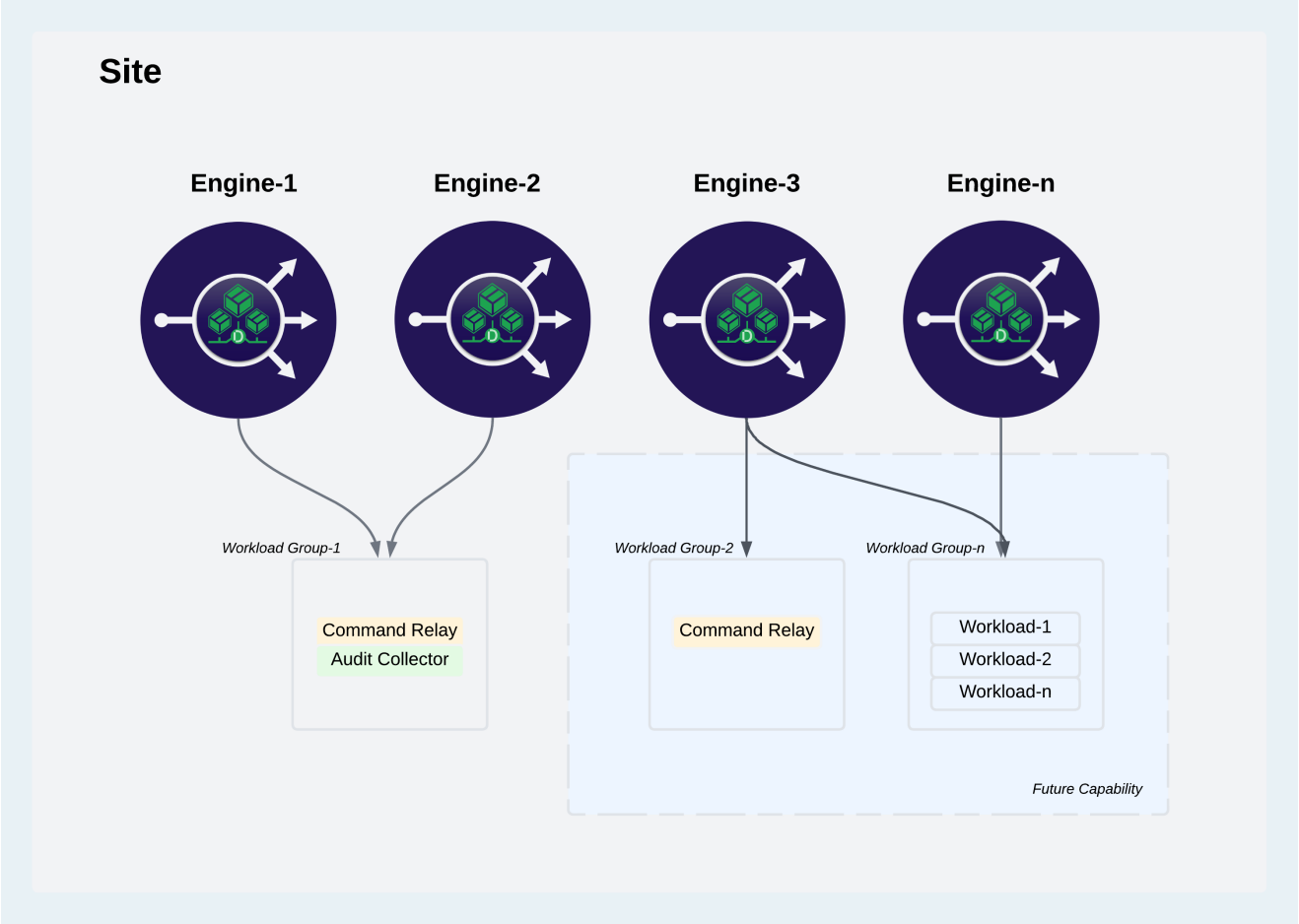
Component	Description
Workload Group	A logical grouping of workloads based on their functional purpose. For example, a group may include database servers and laptops with RAS. All of these have the installed engines. Currently, workload groups are managed in the background. In upcoming releases, administrators will be able to create and adjust these groups, enhancing the level of flexibility. SKS: Will be replaced by workload capabilities
Workload	Workloads are applications that are managed by the engine. They perform functions like facilitating communications between the Platform and downstream assets, capability-specific computations like small or even large scale analytics, pre-processing and collation of data, etc.

Note: The engine and workloads run on a server, but they exchange data with the Delinea platform.

Engine Management Architecture

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.





Engine System Requirements

The system requirements for the server where the Delinea Engine, Command Relay, and Audit Collector are installed are detailed in the table below.

Requirements	Details
Supported Operating Systems	- Windows Server 2022, 2019 - Linux: a modern variant such as Rocky, Alma, Debian
CPU	x86-64 based processors at 2.5 GHz or higher, with two or more cores are recommended for production use
Memory	- For non-production: 2 GB - For production: 8 GB

Requirements	Details
Storage	500 MB or more recommended for installation and run-time needs. **Note**: Logging retention may impact the storage requirements.
Ports	Port 443 (outbound only) must be open for the engine to send encrypted information to the platform via CloudAMQP messaging service. See "Network Communication" on page 258 below.

Outbound Message Queue - Fully Qualified Domain Namess (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 engine to facilitate communication with platform via 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.

US	dramatic-coral-crow.rmq2.cloudamqp.com loud-beige-duckbill.rmq5.cloudamqp.com fast-green-crab.rmq2.cloudamqp.com
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
UK	giant-maroon-bullfrog.rmq3.cloudamqp.com

Notes:
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.

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

Engines retrieve workloads from the Delinea Platform, which supplies securely signed packages for the engine to download.

The engine only runs workload deployment binaries that are both signed and trusted.

During deployment execution, engines maintain 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 re-downloading the deployment packages.

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. Currently, these heartbeats are dispatched every five minutes, ensuring prompt detection of any new updates during this interval.

Engine States

State	Description
Pending	The engine has been installed on a supported OS but has not been approved or 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.
Running	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.
Succeeded	All deployments in the engine have been terminated in success and will not be restarted. This an instruction/state change, i.e. `maintenance mode`
Unknown	The engine state could not be obtained. This phase typically occurs due to an error in communicating with the engine or the machine where this engine should be running.
Failed	All deployments in 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.
None	Uninitialized state

Engine Management Account Permissions and Roles

The table below describes each permission available with an Engine Management Domain Admin account.

Permissions	Description	Permission List	Engine Mgmt. User	Engine Mgmt. 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/create	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
List Sites	Ability to view summary information about all sites	delinea.enginepool/site/list	Yes	Yes
List Workloads	Ability to view summary information about all workloads	delinea.enginepool/workloads/list	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

Permissions	Description	Permission List	Engine Mgmt. User	Engine Mgmt. Admin
List Workload Definitions	The user can read detailed information (including sensitive information) about individual workload-definitions	delinea.registration/workloaddefinition/list	No	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 engines on millions of endpoints per tenant. To achieve high availability and to avoid high load on a web server, 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 is everything from the engine to server. Downstream communication is from the server to the engines. Downstream doesn’t have a gRPC option.

- The engine can get a new configuration from the server passively. It 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.
- Engines always send their heartbeats upstream to the server.
- If the server determines the engine is out of sync, it will then send a message to the groups this engine belongs to. One message from server but the engine that forced that message AND all others that have the wrong group stamp will update. This reduces the load on the bus and engines eventually coalesce. Finally, if an engine stamp itself is outdated, the server will send 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 downstream to the engine its new configuration.
- 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 and will be chosen given 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. Should the message payload exceed 64KB, AMQP protocol is chosen as the message transfer protocol. AMQP uses TLS port 5672.

About Delinea 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 Delinea Engines

An engine functions as a system agent or daemon on an endpoint (server or workstation), to facilitate data exchange with the Delinea Platform. An 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, collector, agent
- **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**: By clicking Add Engine from your chosen engine Site, a PowerShell install script is displayed. Copy and run this script as an administrator to install. Following installation, the engine undergoes registration 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 encompasses 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. This is a future capability.

Managing Engine Sites

Create a Site

1. Click **Settings** from the left navigation menu, then click **Sites and engines** from the secondary menu.
2. Click **Create Site**.
3. Enter a **Site name** and **Description**.
4. Click **Save**.

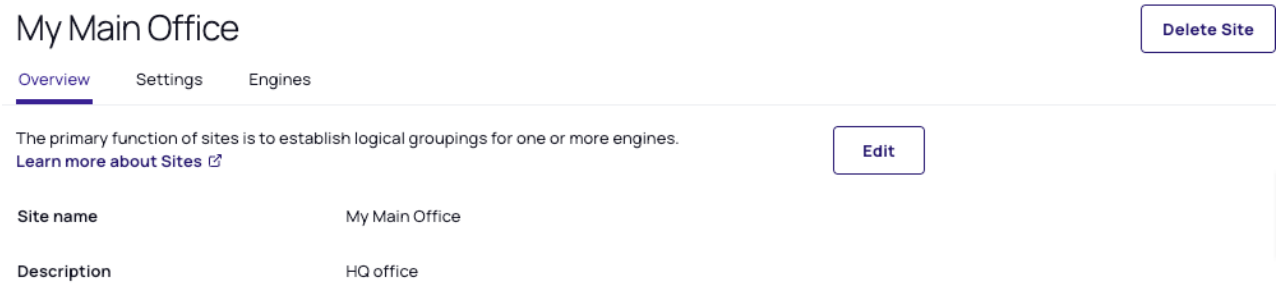
Edit a Site

1. Click **Settings** from the left navigation menu, then click **Sites and engines** from the secondary menu.
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**.

Delete a Site

1. Click **Settings** from the left navigation menu, then click **Sites and engines** from the secondary menu.
2. Select a site.

3. Click **Delete Site**.

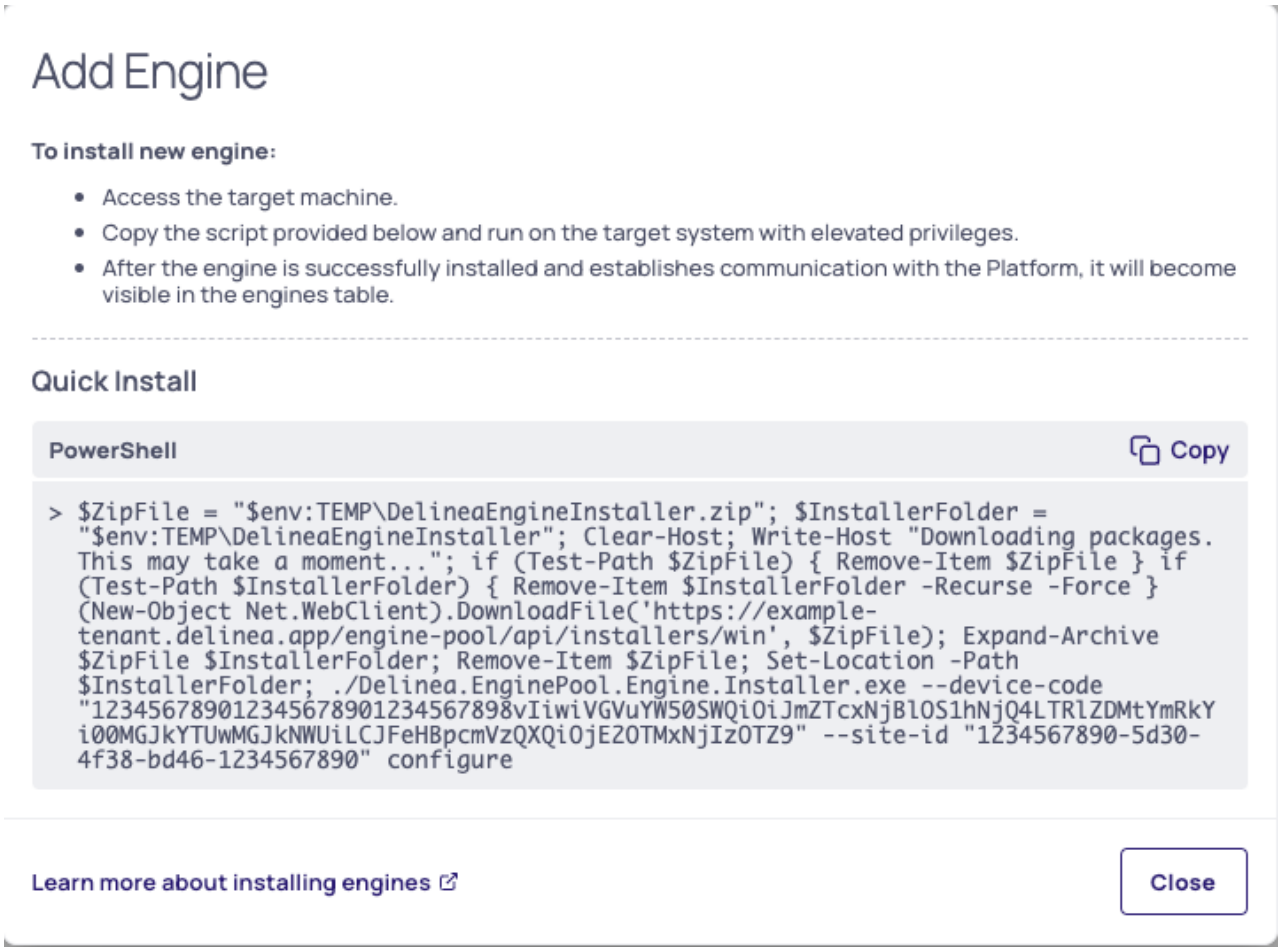


Notes:
- You cannot delete a site that still contains engines. First, remove all engines and then proceed to delete the site. See *Delete Engine*, below.
- You can perform the same action using quick actions in the site table, or using the preview panel.

Managing Engines

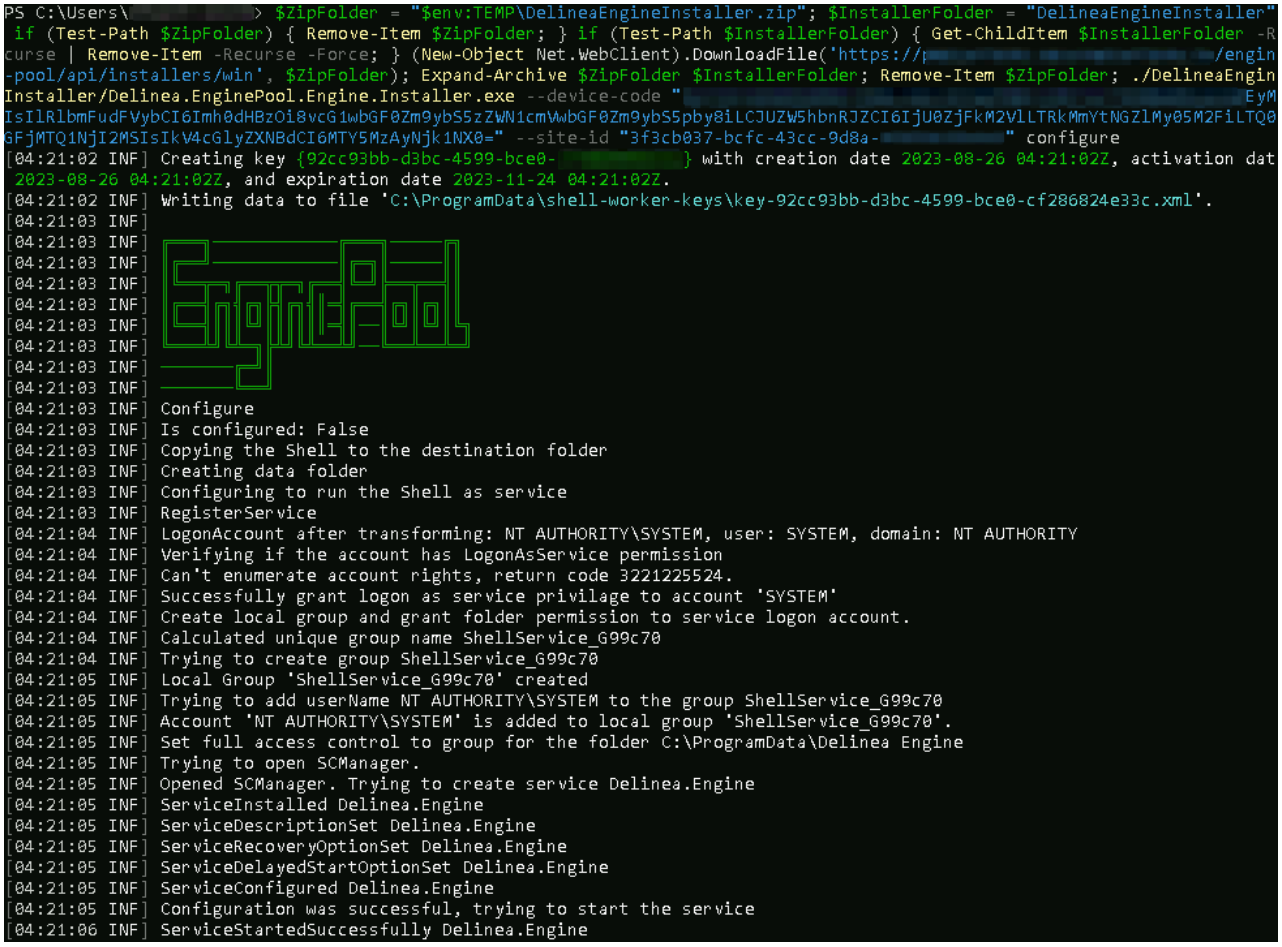
Add an Engine

1. Click **Settings** from the left navigation menu, then click **Sites and engines** 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 **Add Engine.**
5. Click the copy icon to copy the script from the Add Engine dialog. Each time the user accesses the engine installer window, a fresh device code is generated and linked with the script.



6. Access the target system.
7. Copy the PowerShell script provided and run it on the target system with elevated privileges.
8. After the engine is successfully installed and established communication with the platform, it will be displayed in the engines table.

9. The PowerShell script automates the process of downloading the installer and installing the engine.



Automatically Update an Engine

The engines will consistently transmit their state to the platform, encompassing information about active workloads and configurations. Should the platform ascertain that the engine's state has become outdated, it will send an update to the engine. These updates may include settings, workload version updates, or other maintenance directives, including upgrades to the engine itself.

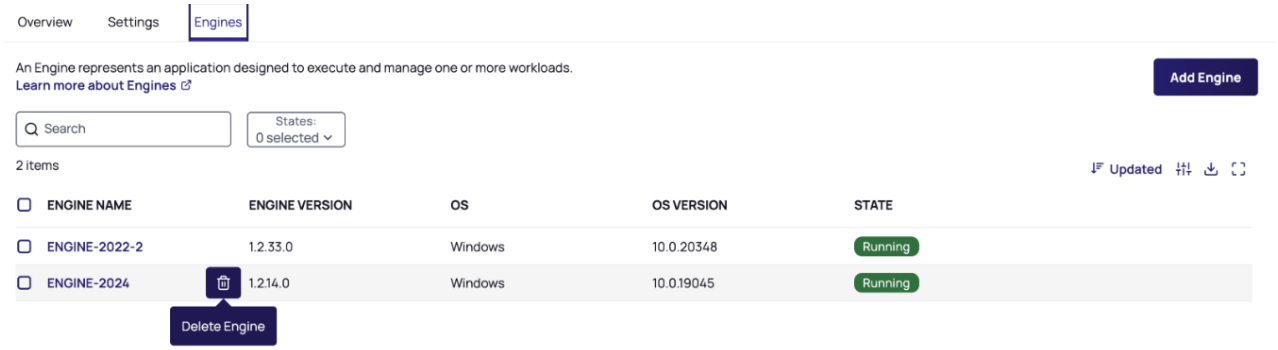
Manually Update an Engine

As of Engine version 1.5.8 automatic upgrades are supported. You should only run a manual upgrade if facing unknown exceptions.

To manually upgrade the engine, follow these steps:

1. Run the PowerShell script as listed above (Uninstall engine from host machine).
2. Navigate to **Sites and Engines**.
3. Open the existing site.

4. Wait for the Engine to uninstall and 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 the *Add Engine* section to add the latest version of the engine.

Uninstall an Engine from the Platform

Uninstalling the engine from the platform will sever its association with the site and remove it from the site list.

1. Click **Settings** from the left navigation menu, then click **Sites and engines** from the secondary menu.
2. Select the site where you want to delete an engine.
3. Click the **Engines** tab.
4. Click the Engine you want to delete.
5. Click **Delete Engine**.
6. Confirm your selection.

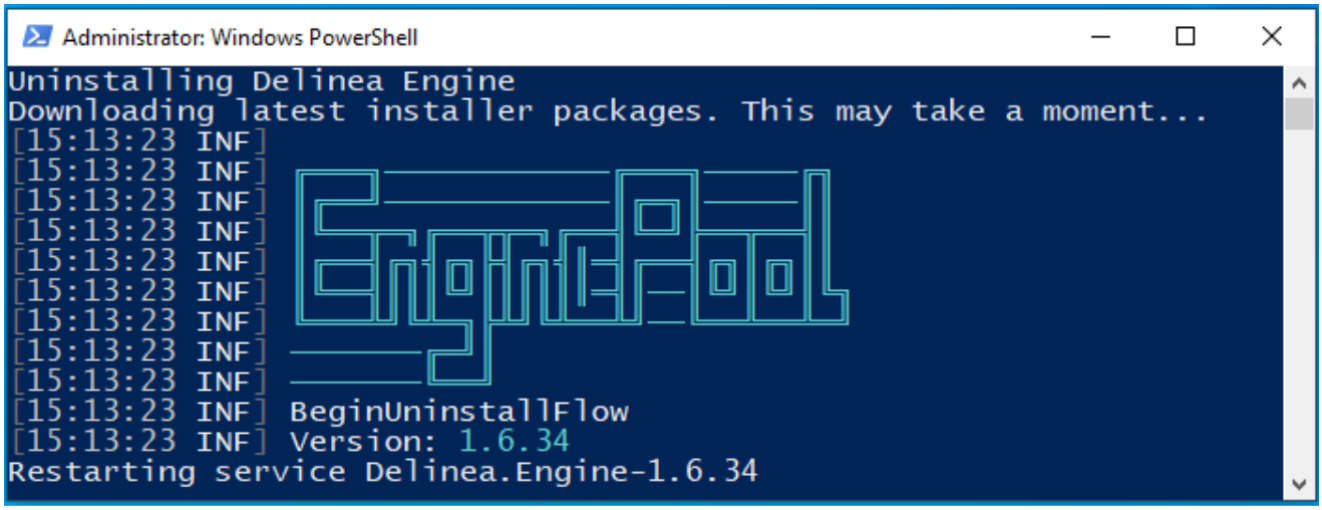
Delete Engine will send an uninstall message to the chosen engine, which will then perform an uninstall on the target machine. You have the option to perform the same delete action directly within the engine's table using quick actions, or through the preview panel. You can also bulk delete engines.

Manually Uninstall an Engine from Host Machine

To completely remove the engine from the host machine, including all Program Files and installed ProgramData, execute the provided command in PowerShell as an administrator. Successful execution should yield a confirmation message, indicating proper completion.

Remove Engine from Host Machine

```
Clear-Host;Write-Host "Uninstalling Delinea Engine";$ZipFile =
"$env:TEMP\DelineaEngineInstaller.zip";$InstallerFolder = "$env:TEMP\$(New-
Guid)";$DataPath = Get-ItemPropertyValue -Path
HKLM:SOFTWARE\Delinea\EngineShell\Installer -Name DataPath;$InstallPath = Get-
ItemPropertyValue -Path HKLM:SOFTWARE\Delinea\EngineShell\Installer -Name
InstallPath;$ProgramDataFolder = Split-Path $DataPath -Parent;$ProgramFilesFolder =
Split-Path $InstallPath -Parent;$VersionName = Split-Path $DataPath -Leaf;$ServiceName =
"Delinea.Engine-" + $VersionName;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 } $Uri =
'https://enginepoolupdatedev.blob.core.windows.net/shell-installer/675160/win-x64.zip';if
($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 --delete-all-
versions;Write-Host "Restarting service" $ServiceName;Restart-Service -Name $ServiceName;
```



Engine and Log Directories

Delinea Engine is installed at
`C:\Program Files\Delinea Engine\[version number]\`

Deployment files and logs can be found here.

After installation and registration, the folders below are created:

Folder	Description
/appdata **/settings**	Contains key file used to encrypt configuration files to discourage manual, machine-level changes. ■ Child folder (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.
/log	Contains engine runtime logs. This folder contains Registration, Bootstrap, and Default logs. Bootstrap and Registration record engine start-up and registration logs. Default log contains process logging: including updates from the platform's Engine Management service, starting and ending deployments, and sending heartbeats to Platform. This folder may also contain a SelfUpgrade log when a new version is made available and the engine starts, which when detected, will install the new version. If engine detects an Uninstall config file, it will automatically shut down and uninstall itself.
/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 deployment folders used for temporary processes such as downloading and extracting deployment installations. ■ Contains folders for each deployment. • Each deployment has versioned folders which contain: ◦ Settings folder ◦ Logs folder ◦ Deployment state encryption key

Engine Logs

The current log levels for various components are found under **LogLevel and MinimumLevel** to the right of the respective component. These values can be changed to other values on the table below. Each level includes the levels below it. For example, if the level is set to **Warning**, messages at the **Error** level will also be 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 existing values 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.

Adjust Engine Log Levels

To change the engine log level, open `C:\Program Files\Delinea Engine\[version number]\appsettings.json` in a text editor with administrator privileges.

After setting the desired log levels, save `appsettings.json`. If the save is not successful, make sure you are running your text editor with administrative privileges.

Restart the engine service through the operating system services manager.

Workloads

At its core, a workload is an application that runs a continuous task such as a background service. Workloads can have various versions, known as deployments. Two workloads that run on the engine are Audit Collector and Command Relay, described is sections below.

- **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.
- Deployments are akin to versions or editions of a workload. Each workload's engine will run just a single deployment.

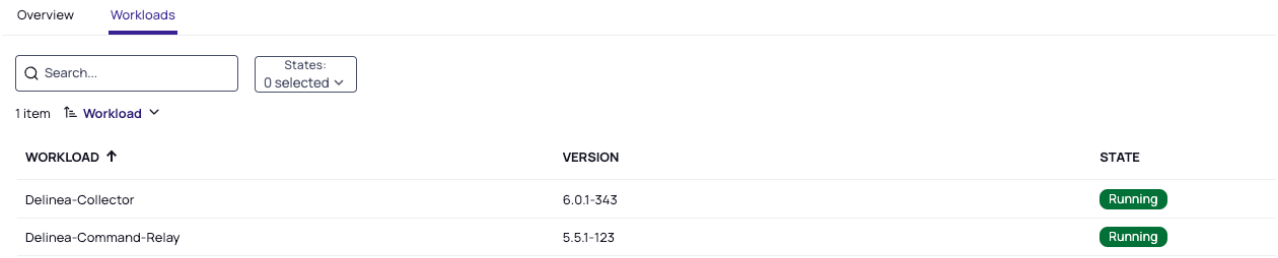
Workload Deployment States

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.

State	Description
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. That is, the entry-point either exited with non-zero status or was terminated by the system.
Unknown	For some reason, 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 deployment was not selected by the engine to be run.

Monitor Workloads

1. Click **Settings** from the left navigation menu, then click **Sites and engines** from the secondary menu.
2. Select a Site.
3. Click the **Engines** tab.
4. Select an engine.
5. Select the **Workloads** tab.



Note:
Individual workload logs are kept in the **deployment** directory:
C:\ProgramData\Delinea Engine**deployment**

For instance, logs for the Delinea Collector are located here:
C:\ProgramData\Delinea Engine**deployment**\authorization\Delinea-Collector\[version]\log

Delinea Audit Collector Workload

Audit collectors send audit data to the Delinea Platform, allowing for the presentation of recorded activities and events.

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 and/or improved scale. 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 and subsequently transfers it to a collector once the connection is reestablished. The collector then transmits this data to the Delinea Platform.

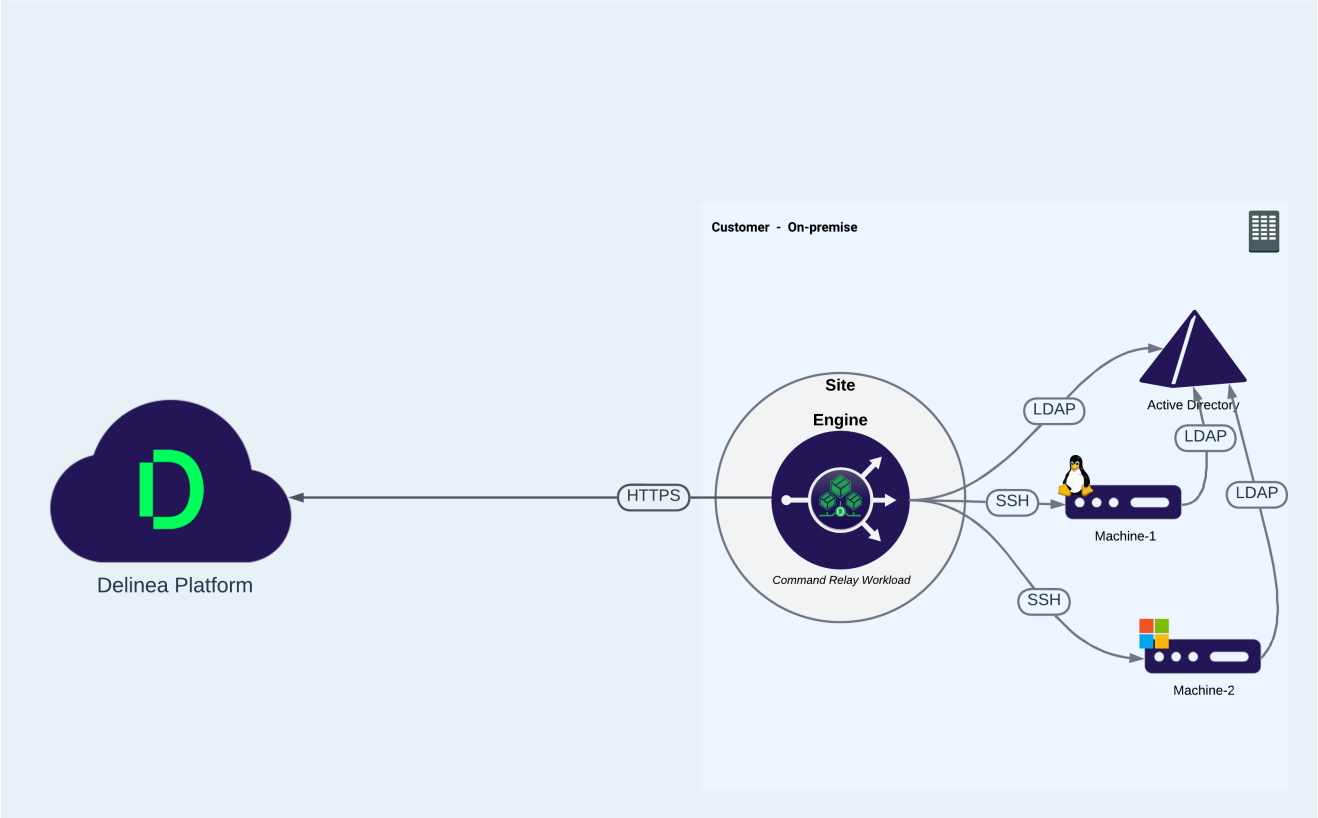
Edit Audit Collector Settings

1. Click **Settings** from the left navigation menu, then click **Sites and engines** from the secondary menu.
2. Select a site.
3. Click the **Settings** tab.
4. Click **Edit** to type 'Enabled or 'Disabled' for Session Recordings to Platform, or to 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

Command Relay Workload

The command relay 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 Engine target machine.

> **Note:** If .Net 4.8 is not already installed, Command Relay will install it automatically, and you will need to reboot the server.

Command Relay activates the PowerShell module on the Windows Server machine, and it downloads and installs the PoweShell feature required by Command Relay.

Edit Command Relay Settings

To execute the Command Relay workload, a Domain Admin 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 **Sites and engines** from the secondary menu.
2. Select a site.
3. Click the **Settings** tab.
4. Edit the Command Relay settings.
5. The Command Relay Domain Account will show 'None' for the first time.
6. Click **Select** for Command Relay Domain Admin Account.

7. Search for the vaulted account where you have permissions.
8. Select **Turn off folder inheritance and Share Secret**. This action will disable inheritance, granting workloads access to the secrets.
9. Click **Save** once the domain is selected.

Setting	Description
Domain	User should be able to select the Domain accounts they already have access too

Command Relay Account Permissions

On the server where you will install the Delinea 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.

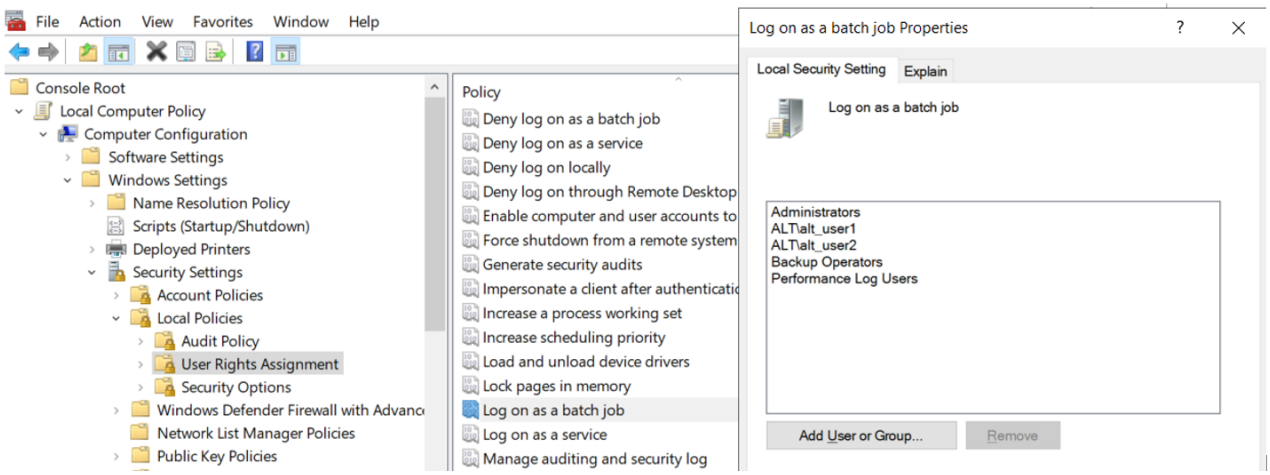
Local Server Permissions

With local permissions on the server where the Delinea 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. Navigate to: **Local Computer Policy** > **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **User Rights Assignment**.



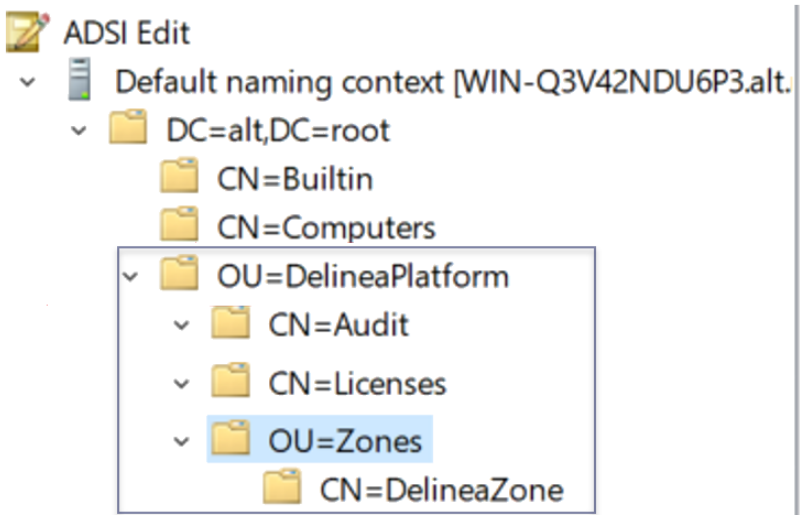
2. Select the **Log on as a batch job** permission.
3. On the Local Security Setting tab, click **Add User or group...**
4. Navigate to and select the Command Relay service account to apply the permission.

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

With domain permissions, the Command Relay service account can manually create the DelineaPlatform OU and all sub-containers needed for Command Relay, including the DelineaZone container. The container structure where domain permissions are applied is shown in the multi-level list below, and in the Active Directory Users and Computers screen shot below that:

- OU=DelineaPlatform
  - CN=Audit
  - CN=Licenses
  - OU=Zones
    - CN=DelienaZone



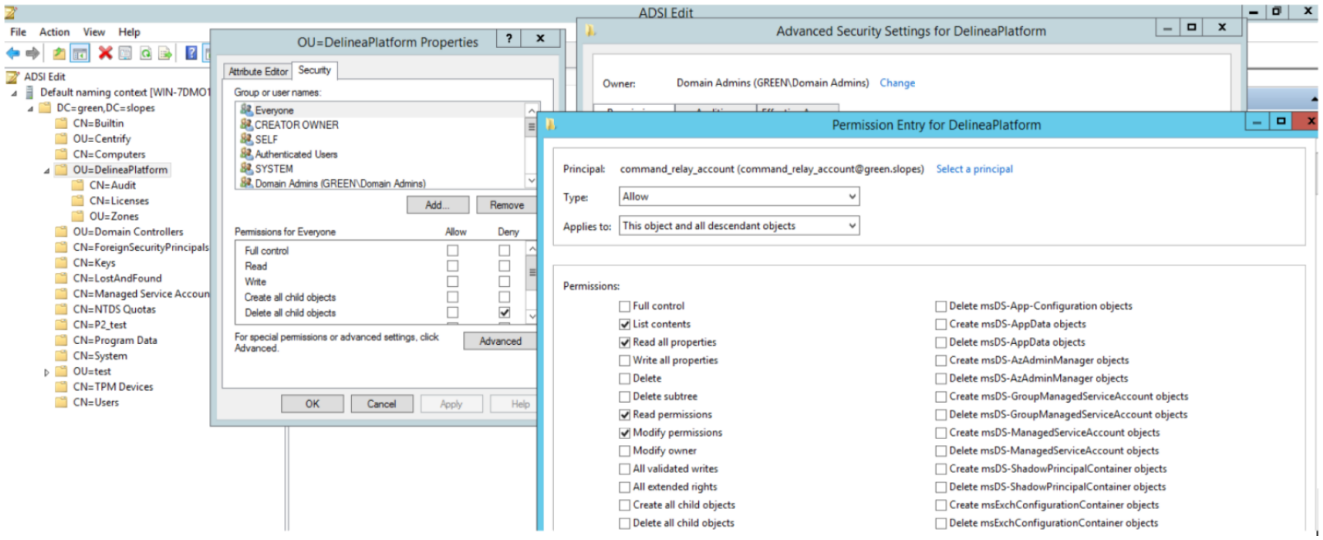
The DelineaZone OU will hold all the agent policies that must be enforced on applicable servers. The DelineaZone is managed by the platform.

Grant domain permissions to the Command Relay service account

To grant domain permissions to the Command Relay service account, follow these steps (use the ADSI edit tool instead of ADUC):

1. Right click the OU=DelineaPlatform container
2. Click **Properties**.
3. Click **Security**.
4. Click **Advanced**.

5. Click **Add**.
6. Next to Type, select **Allow**.
7. Next to Applies to, select **This object and all descendant objects**.
8. Use the ADSI edit tool (not the ADUC tool) to select the boxes next to the following permissions:
   - List contents
   - Read all properties
   - Read permissions
   - Modify permissions
   - Create classStore objects
   - Create Container objects
   - Create Organizational Unit objects
   - Create serviceConnectionPoint objects



Domain Admin Permissions (temporary)

> **Important:** For security reasons, Delinea recommends ***not*** leaving Domain Admin permissions on the Command Relay service account

If you temporarily assign comprehensive Domain Admin permissions to the Command Relay service account and install the Delinea Engine, Audit Collector and Command Relay are also installed, and the DelineaPlatform OU is set up automatically along with all required subcontainers.

Temporarily assign Domain Admin permissions to the Command Relay account

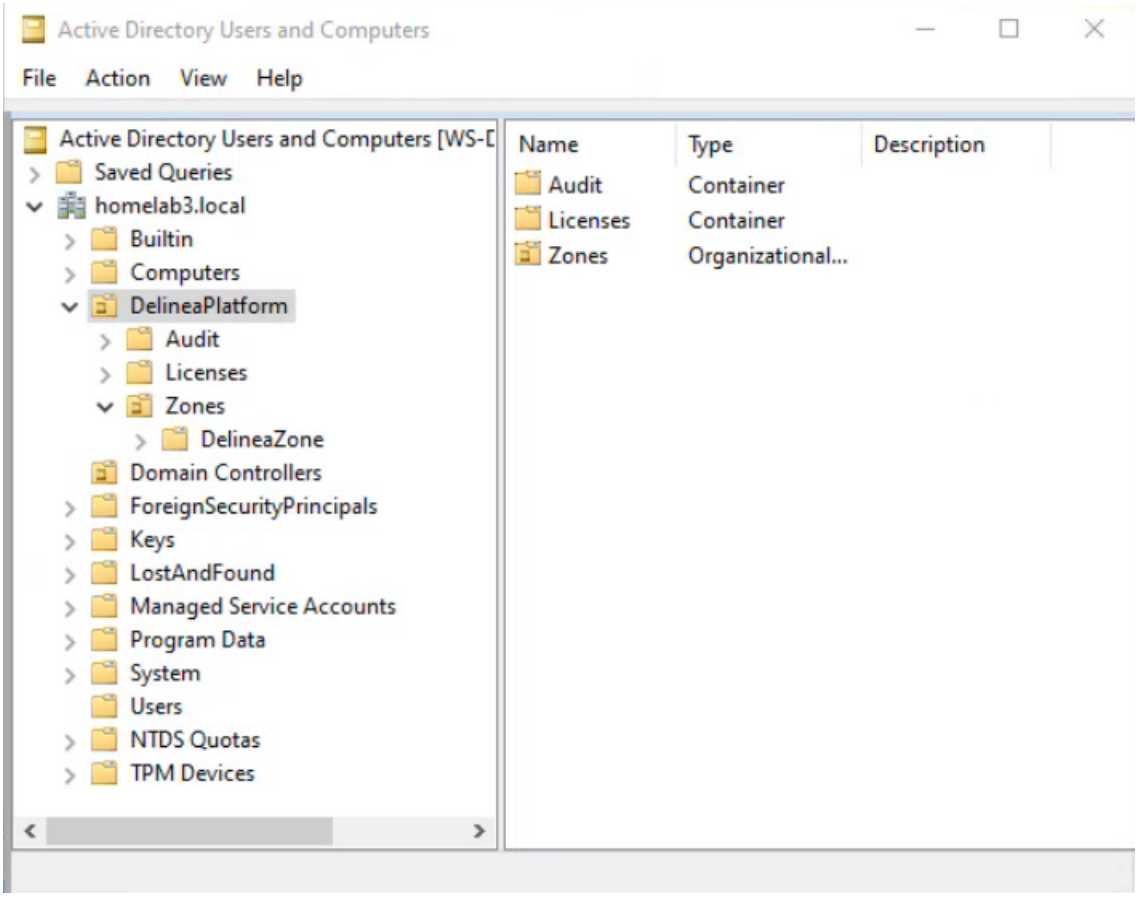
1. To temporarily assign comprehensive Domain Admin permissions to the Command Relay service account, simply add the service account to the **Domain Admins** group.
2. Log into the server as the Command Relay service account with temporary Domain Admin permissions.

3. Install the Delinea Engine.
4. Add the Command Relay service account to either the **Backup Operators** group or the **Performance Log Users** group. The account will inherit the **Log on as a batch job** permission through membership in these groups.
5. Remove the new Command Relay service account from the **Domain Admins** group.

> **Note:** If you do not want to assign the Command Relay service account to the Backup Operators group or the Performance Log Users group, you must grant the **Log on as a batch job** permission to the account manually, as described under "Local Server Permissions" on page 271.

The DelineaZone

When Command Relay executes, it creates the DelineaZone within the DelineaPlatform OU, as shown in the image below.
The DelineaZone contains all the agent policies that need to be enforced on applicable servers. The DelineaZone is managed by the platform.



Minimal Permissions to Join a Server to a Zone

On Windows

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

On *nix

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

Engine Troubleshooting Guide

Issue: Engine does not appear, is outdated, or status shows “failed”

Resolution: Investigate engine-specific logs here:

`C:\ProgramData\Delinea Engine\<engine_version>\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

Issue: Engine upgrade problems

Note: Beginning with engine version 1.4.3, if you have an existing installed engine, engine will recognize updates are available and will upgrade itself automatically. Manual upgrades are no longer necessary.

Resolution:

Check this path for engine-specific logs: C:\ProgramData\Delinea Engine\<engine_version>\log

If a `Delinea.Engine.SelfUpgrade.[date].log` 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 5-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 section below.

Issue: Need to manually reinstall engine

Resolution: Open PowerShell ISE or Powershell.exe as administrator and run the script located at "Manually Uninstall an Engine from Host Machine" on page 264.

1. 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}
2. Wait for the engine to uninstall.
3. Go to your tenant portal under **Sites and Engines** and make sure the engine disappears.
4. Select the Site for the engine you are reinstalling.
5. Click **Add Engine** and copy the full Quick Install script.
6. Run the script in PowerShell ISE or Powershell.exe as administrator.

Issue: Workload status shows “failed”

Resolution:

Command Relay: Command Relay records logs in two places.

- Engine management stores runtime logs here: `C:\ProgramData\Delinea Engine\<engine_version>\delinea\command-relay\<workload_version>\log`
- Command-Relay detailed logs can be found here: `C:\ProgramData\Delinea\CommandRelay\Logs`

Audit Collector: `C:\ProgramData\Delinea Engine\<engine_version>\delinea\audit-collector\<workload_version>\log`

Issue: Selected secret (domain admin account) for Command Relay stopped working

Resolution:

Command Relay

Command Relay could stop working if the sharing on the secret is changed, e.g., if you move the secret to a personal folder in Secret Server after it is selected, it will remove the Delinea Workload Service shared permissions on the secret which will cause permission failure in Command Relay.

> In this scenario, simply reselect the secret through Site > Settings > Command Relay > credential secret picker. Save to update permissions and reshare the secret with the workload.

Command Relay may also experience issues if the underlying domain account associated with this secret is changed, e.g., password expired/not synced, account locked, AD permissions removed, etc.

> In this scenario, check the Command Relay-specific logs to find log on failures with error details.

Issue: Getting 400s when engine is trying to register

Resolution:

1. Verify that time in domain is accurate. If the ntp service on hosts isn’t running, the time in the domain will be a few minutes off.
2. Reconfigure the ntp service and sync the domain controller

Appendix: Engine and logs directory structure

The Delinea Engine is installed here:
`C:\ProgramData\Delinea Engine\[version number]\.`
Deployment files and logs can be found here.

After installation and registration, the folders below are created:

Folder	Description
/appdata **/settings**	Contains key file used to encrypt configuration files to discourage manual, machine-level changes. ■ Child folder (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.
/log	Contains engine runtime logs. This folder contains Registration, Bootstrap, and Default logs. Bootstrap and Registration record engine start-up and registration logs. Default log contains process logging: including updates from the platform's Engine Management service, starting and ending deployments, and sending heartbeats to Platform. This folder may also contain a SelfUpgrade log when a new version is made available and the engine starts, which when detected, will install the new version. If engine detects an Uninstall config file, it will automatically shut down and uninstall itself.
/metadata	Contains information used to verify the integrity of deployment installations. Contents of this directory must not be modified.

Folder	Description
/deployment	delinea\<deployment name>\<version>\ ■ Contains deployment folders used for temporary processes such as downloading and extracting deployment installations. ■ Contains folders for each deployment. • Each deployment has versioned folders which contain: ◦ Settings folder ◦ Logs folder ◦ Deployment state encryption key

Inventory

The platform Inventory service provides a user-friendly, asset-centric view of all computer assets discovered using the Secret Server discovery service in one place—the Inventory page. From there you can efficiently manage your computer assets and initiate remote sessions directly on them. To learn more about Secret Server's discovery service, see Secret Server Discovery.

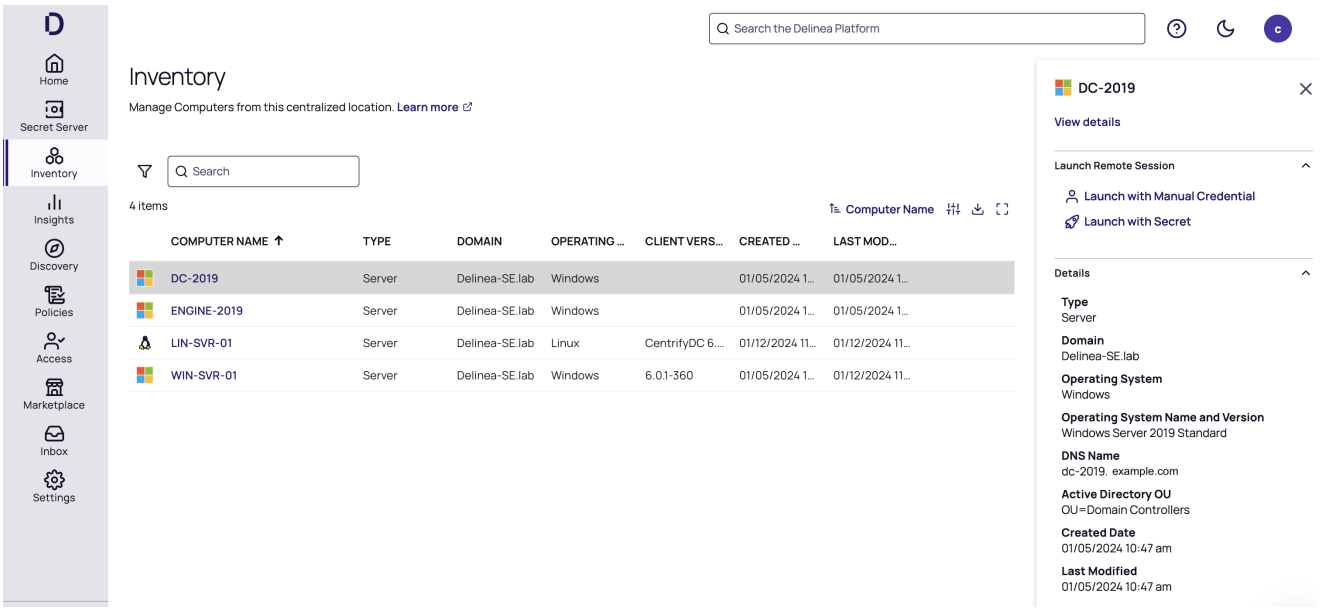
Note: Currently, the default platform user role does not provide permissions to view inventory. An administrator must create a custom role with permissions to view the inventory (View Computers - delinea.assets/computer/view) and launch RAS sessions into the assets, and then assign the role to appropriate users and groups.

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

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

Viewing Your Platform Inventory

Once Secret Server discovery has been enabled and configured, you can view your inventory through the platform interface by selecting **Inventory** from the left navigation panel. 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.



If you click any empty space in a computer asset row, a panel opens on the right side of the page displaying basic asset information and options to **View Details** and **Launch with Credentials**.

Launching into a Computer Asset

To launch into a computer asset, hover your cursor over the computer's name column and click the launch (rocket) icon, then click one of the three launch methods: **Use My Account**, **Manual Login**, or **Vaulted Credential.**

You can also launch into a computer asset by clicking any empty space in the computer's row and then clicking one of the three launch methods.

Launch (Login) Options

Launch with Manual Credentials

Selecting Manual log on allows users to launch manually 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 an additional authentication challenges before logging on.

Launch with Use My Account

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

Launch with Secret

You can log on to any target system in 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.

Disabling Inventory

To deactivate 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

You can assign precise machine-level policies tailored to match your compliance requirements, ensuring that each asset operates securely and efficiently within your infrastructure. To learn more about assigning machine level policies, see PCS Policies.

Using Secrets

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. 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.

Secret Server Overview

Delinea Secret Server is an enterprise-grade solution for privileged access management (PAM), designed to help organizations securely store, manage, and control access to privileged credentials. It aims to improve the security of sensitive data, reduce the risk of data breaches, and streamline the password-management process.

Secret Server Cloud (SSC) is a scalable, multi-tenant cloud platform hosted on the Microsoft Azure infrastructure. All backend services, databases, and redundancy are securely managed by Delinea. Customers do not have direct access to the databases or application file system.

Secret Server is also available as an on-premise solution named Secret Server On-Premise.

Secret Server Documentation for New Users

Secret Server Cloud also has its own complete documentation set. The information at the following links is specifically relevant to new users:

- Secret Server Cloud Quick Start (an orientation for new administrators) Secret Server Cloud Quick Start
- End User Guide (a guide for non-administrator users)

Secret Server Key Features

- **Secure Password Storage**: Secret Server stores privileged credentials in an encrypted format, protecting sensitive information from unauthorized access.
- **Access Control**: Secret Server implements role-based access control, allowing administrators to set permissions and control who has access to sensitive information.
- **Privilege Escalation Management**: Secret Server integrates with Windows systems to provide privilege escalation management, helping to reduce the risk of data breaches.
- **Auditing and Reporting**: Secret Server provides detailed audit logs and reports, making it easier for organizations to track access to sensitive information and detect any unauthorized activity.
- **Automated Password Management**: Secret Server supports automated password management, helping to streamline the password management process and reduce the risk of manual errors.
- **Multi-Factor Authentication**: Secret Server supports multi-factor authentication, helping to improve the security of sensitive information.
- **Integration with Other Tools**: Secret Server integrates with a variety of other tools, including Active Directory, Microsoft Azure, and cloud-based applications, making it easier for organizations to manage their passwords and access controls.

Secret Server Secrets

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)
- Creating Secrets
- Secret Configuration Options
- Editing Secrets (includes manually changing passwords, instead of waiting for expiration)
- Deleting and Undeleting Secrets

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. For more information about secret folders, see the following:

- Creating Folders
- Adding and Moving Secrets Between Folders

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:

- Secret Checkout.

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:

- Discovery Overview
- How Discovery Works
- 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.

For more information about distributed engines, see the following:

- 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:

1. Advanced Session Recording: Secret Server captures all user activity during privileged sessions, including commands entered, files accessed, and changes made to the system or application. This provides a detailed record of user activity, enabling IT teams to investigate security incidents and respond quickly to potential threats.
2. Audit Logs: Secret Server logs all activity related to privileged accounts and credentials, including login attempts, password changes, and access to sensitive data. This provides a complete audit trail of all privileged activity, enabling organizations to comply with regulatory requirements and industry standards.
3. Advanced Search and Filtering: Secret Server provides advanced search and filtering capabilities, enabling organizations to quickly find specific events or actions in audit logs. This saves time and helps IT teams to identify potential security risks or incidents more efficiently.
4. Alerting and Notifications: Secret Server enables organizations to configure policies to automatically alert administrators when specific events occur, such as failed login attempts or changes to system configurations. This helps organizations to respond to potential threats in real time.
5. Reporting: Secret Server provides a range of built-in reports, enabling organizations to generate customized reports on privileged account activity, user behavior, and compliance. This helps organizations to track progress and identify areas for improvement.

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 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 via email, SMS, or through a third-party system, and can set up different alerts for different users or groups. This helps organizations to respond to potential security threats in real-time and ensure that their privileged accounts and credentials are being used appropriately.

- Inbox
- Event Subscriptions
- Event Pipelines

Built-in Reports

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

- Configuring Session Recording
- Built-in Reports

Remote Access Service

The Delinea Remote Access Service (RAS) 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 RAS 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. RAS automatically uses credentials to connect with target resources, enabling RDP and SSH connectivity without exposing sensitive parts of credentials to the end-user. This fast and simple workflow is completely integrated into the Delinea Platform UI.

Delinea RAS displays RDP and SSH sessions in the user's web browser, freeing users from needing to install and maintain additional remote access or VPN software. This architecture also makes RAS extremely portable, enabling the user to access multiple connections to multiple target systems, each running on its own tab in the user's browser.

The Delinea RAS service runs in the Delinea cloud and enables VPN-less connectivity to target systems using the Delinea RAS Engine, which has a small footprint and runs on a variety of Linux distributions in the customer's data center. RAS Engines connect outbound from the customer's datacenter to the Delinea cloud using Transport Layer Security (TLS) over HTTP/S. This technique eliminates the need for a VPN as well as protects from exposing any system to limit threats like port scans and similar malware.

RAS Sites logically group together engines that can facilitate connections to a common set of target resources. Customers have the option of adding multiple engines at each site for redundancy and high availability.

When a user requests a connection to a remote resource, they connect to the Delinea Platform first with their browser using TLS over HTTP/S. Delinea RAS then connects them with the RAS engine thus providing end-to-end protection from the user's browser into the RAS Engine. The RAS engine is also used to integrate on-premises Secret Server installations to the Delinea Platform.

RAS Engines are easy and quick to deploy (in minutes usually) and can easily be managed from the Delinea Platform UI. Updates are delivered from the platform on-demand without interrupting existing user sessions. Engine updates are simple deploy and take just a few seconds, enabling customers to keep their engines at peak performance and up-to-date with no downtime.

For additional security, RAS sessions can be configured to be viewed in close-to-real time and recorded for security auditing.

Continue to Setting Up RAS.

Setting Up RAS

The content in this section is intended for tenant administrators of the Delinea Platform managing RAS sites and engines. It provides the requirements for setting up RAS on the platform, instructions on how to add secret templates to RAS, how to set up a RAS engines site, and how to install, activate, and uninstall RAS engines.

Other sections provide instructions for RAS user tasks, and for RAS session recording.

Continue to RAS Requirements.

RAS Requirements

Delinea RAS runs in the Delinea cloud and connects to target servers using the Delinea RAS 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 7+ and Ubuntu 18.X+.

  Note: RAS only supports operating systems that have not reached their official End-of-Life date. For best performance and compatibility, we highly recommend deploying RAS 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
- **Storage**: 100 MB or more recommended for installation and runtime needs
- **Firewall Rules**: 443 TCP Outbound Open

- **Network**: The RAS engine will function as long as the remote target server or Secret Server On Premises can be found via an IP address or DNS lookup and is reachable on the Local Area Network or via routing tables.
- **Supported Web Browsers**:
  - Google Chrome
  - Mozilla Firefox
  - Microsoft Edge Chromium. Legacy Microsoft Edge is not supported.
  - Safari

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 Remote Access Service with Secret Server on-premise, please refer to "Manually Integrate Secret Server On-Premise" on page 30

Useful Tools

The following tools are not necessary to run a RAS engine, but may be useful with troubleshooting if needed:

- netstat
- journalctl
- telnet
- netcat
- df
- top
- free
- vmstat

Sizing Guidance for RAS Engine Linux Hosts

The RAS engine runs on supported Linux hosts (for more information, see "RAS 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 RAS service in the Delinea Platform selects a single RAS 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 RAS engine depending on the number of concurrent RAS session that engine needs to host.

Size testing was performed on RAS 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 RAS engine, as well as a site associated with two RAS 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:

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 RAS 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 RAS 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 RAS as compared to running vim to edit a text file on a remote SSH session. Performance test data also indicates that RAS 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 RAS engine and the target server also affects the user-experience.

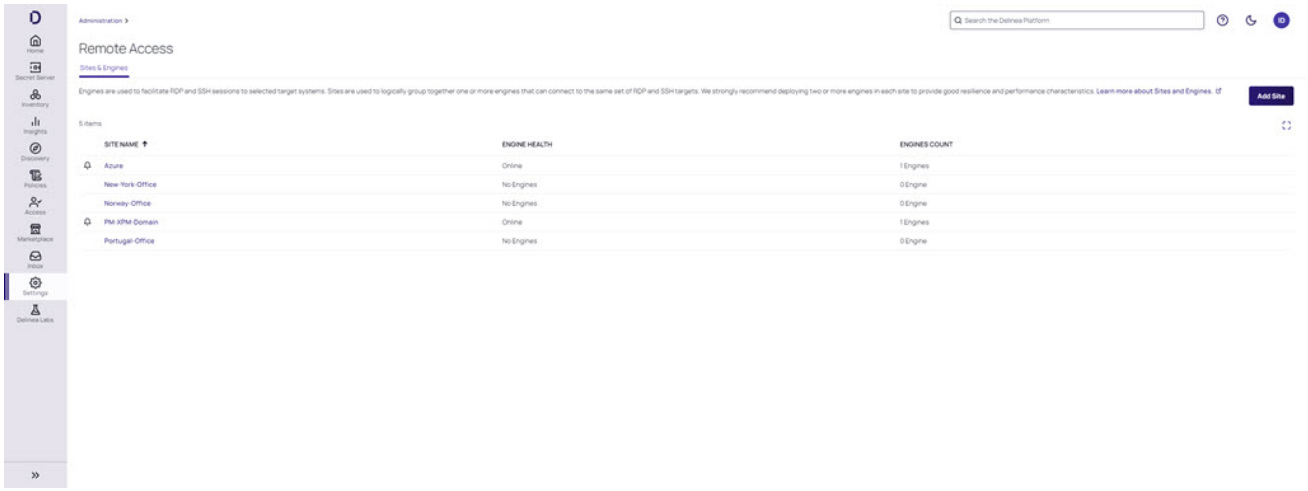
We recommend the following steps when experiencing RAS performance issues that may be associated with RAS engines:

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 RAS engine and the Delinea Platform tenant.
   b. The RAS engine and target machines
4. Contact Delinea Support.

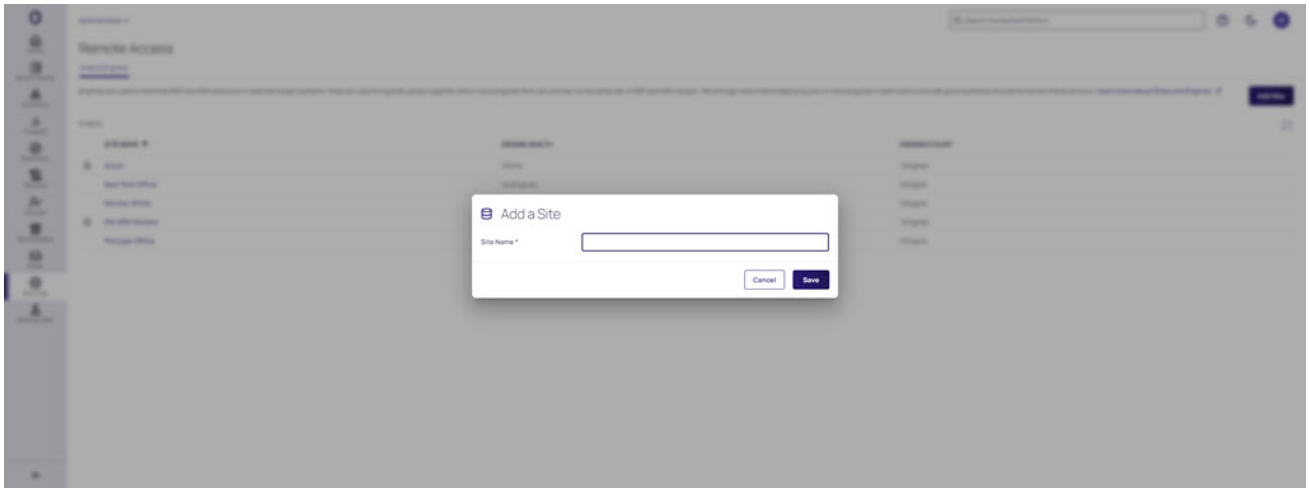
Set Up a RAS Engines Site

1. SSH into the on-premises server where you would like to install the RAS engine, and log in with administrative privileges.
2. From the left navigation menu, click **Settings**, then click **Remote access**. The **Sites & Engines** tab will appear..

3. On the **Sites & Engines** tab, Click the **+Add Site** button.



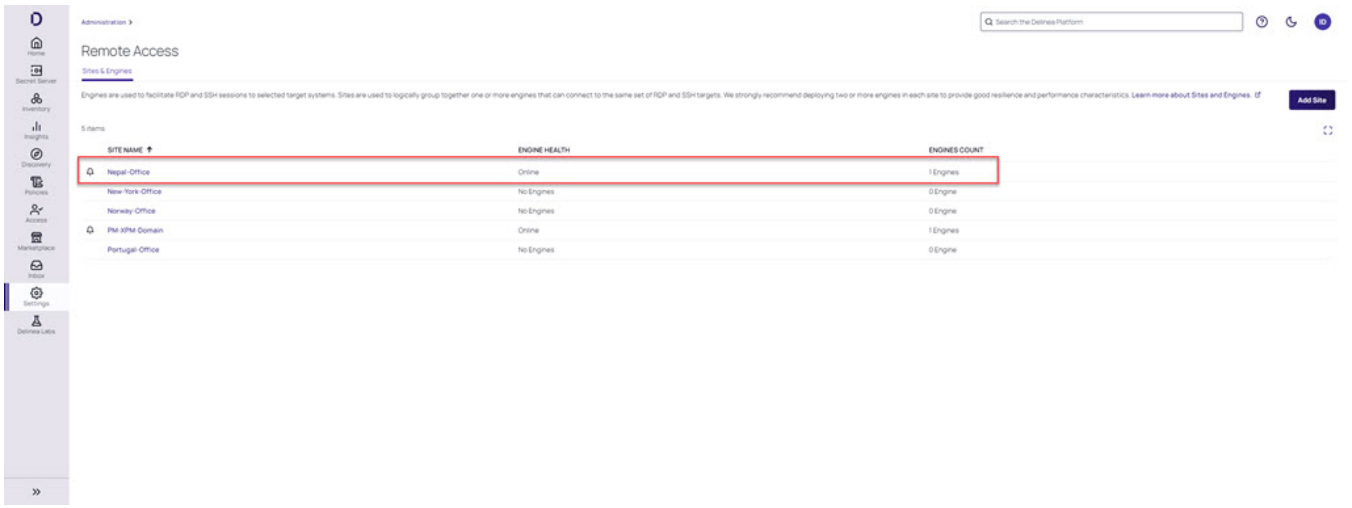
4. On the **Add a Site** page, enter a descriptive Site Name, for example `Secret-Server`. You can use only letters, number, hyphens, and underscores in the name.

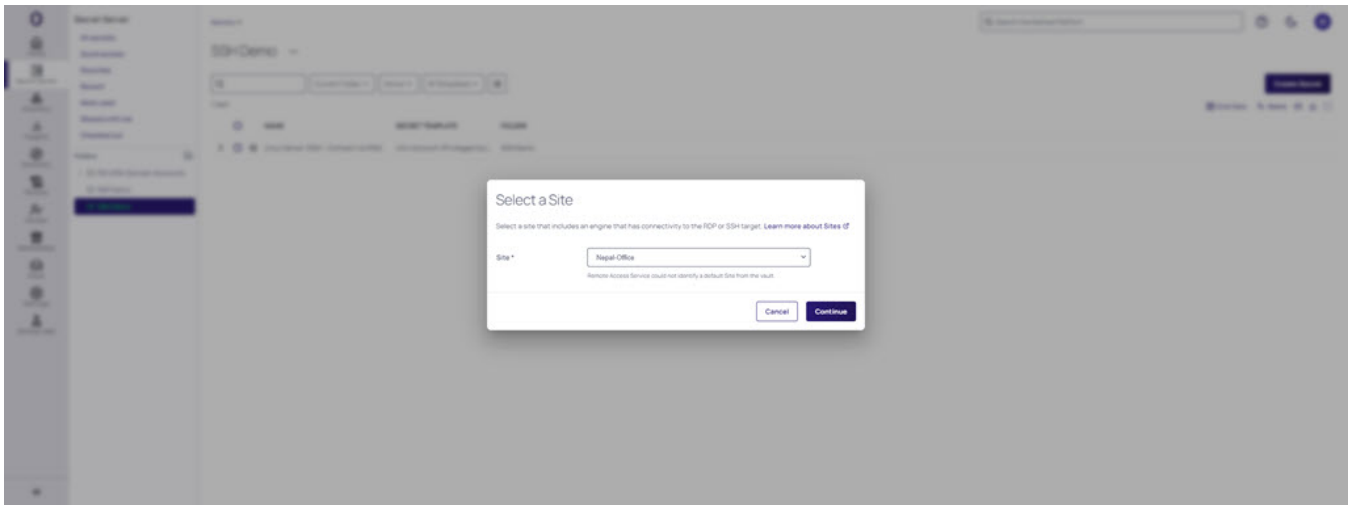


5. Click **Save**.

Naming a RAS Site

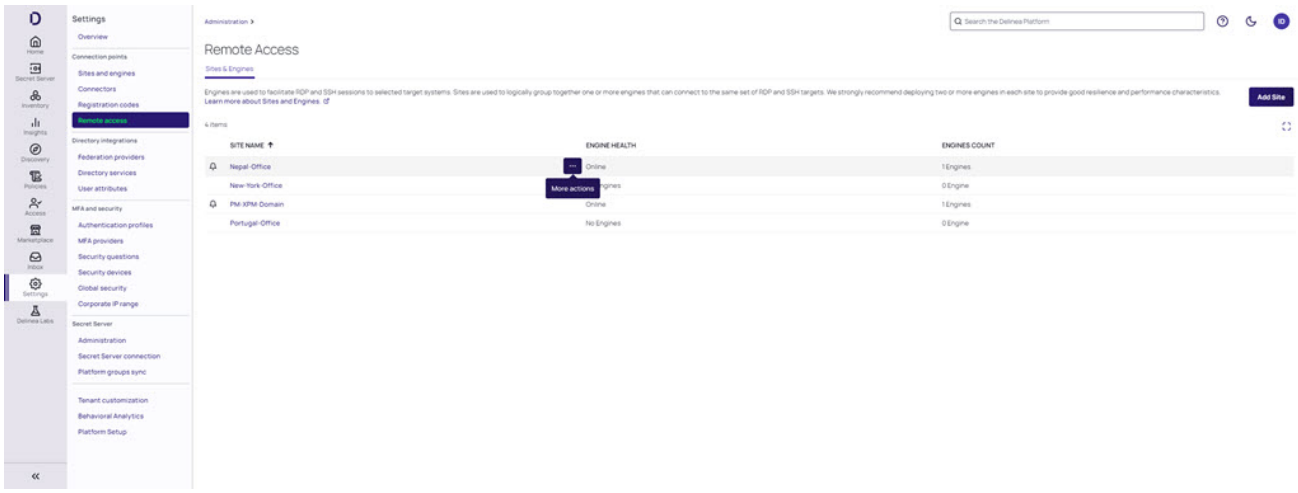
Delinea recommends that tenants use the same name for both RAS Engine Sites and Secret Sites. This way, when a user selects a secret, the preferred RAS Engine Site is automatically pre-selected when launching that session. Without this practice, users would have to manually select a RAS Site and may select the wrong one.



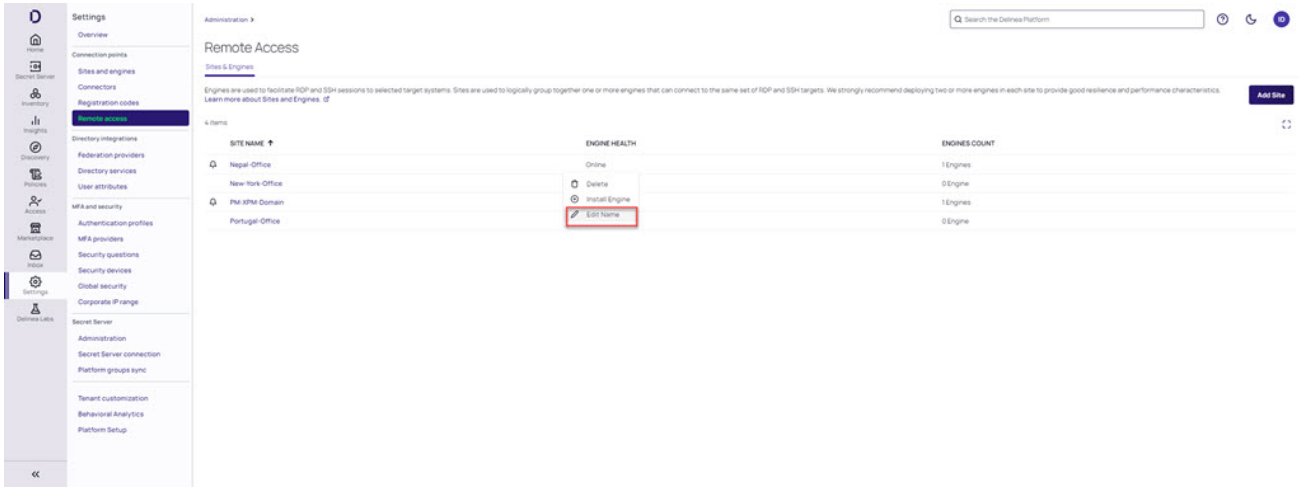


Renaming RAS Site

1. From the left navigation menu, click **Settings**, then click **Remote access**.
2. Click the **More Actions** menu next to the site name.

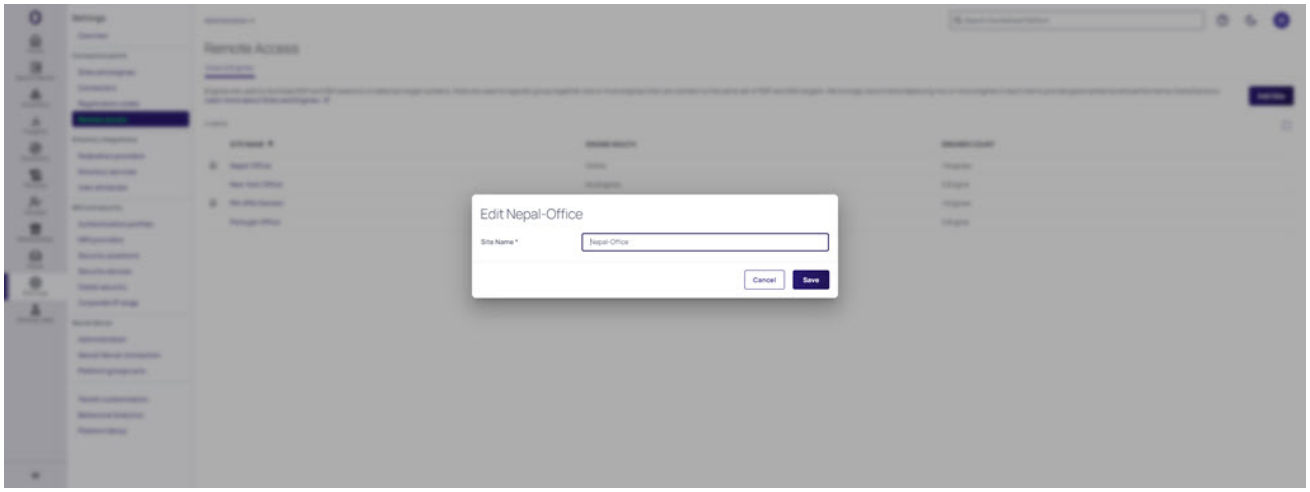


3. Click **Edit Name**



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.

5. The *Edit Site Name* dialog box will appear



6. Enter the new name of the RAS site
7. Click **Save**

> **Note:** If the save fails, an error message will be displayed explaining the cause of the error.

Install RAS Engines

Engine Rules

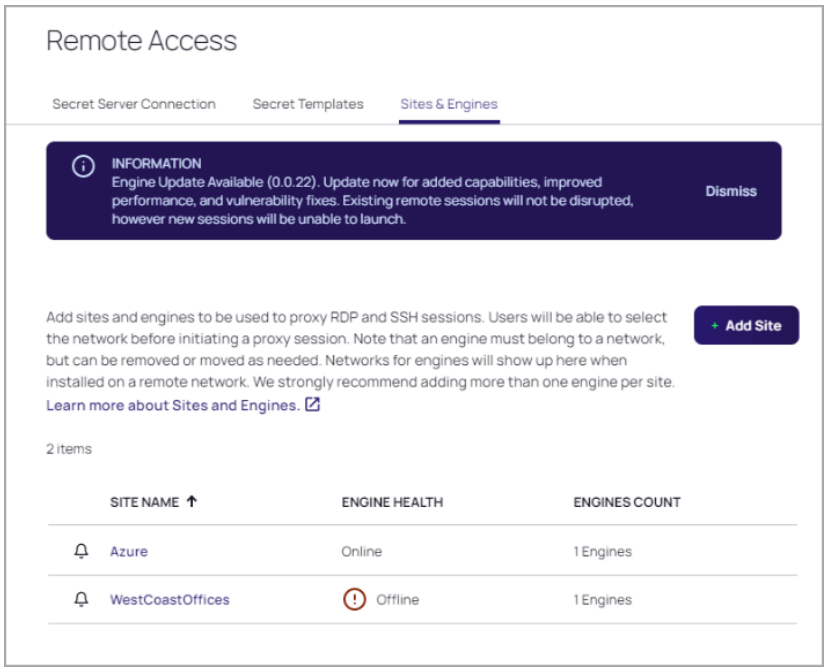
- You must first set up a Site before you can install a RAS engine. See Set Up a RAS Site for options with detailed instructions.
- Only one RAS engine may be installed on any given on-premise RAS server.
- We strongly recommend installing at least two RAS engines per site.
- Engine names must be unique per site.
- Engine names can contain only letters, numbers, hyphens, and underscores.
- While an engine is in the process of updating, existing RAS sessions will continue uninterrupted. However, new sessions will be unable to launch on the engine until the upgrade is complete.

> **Note:** Please review the RAS Requirements for servers hosting a RAS engine.

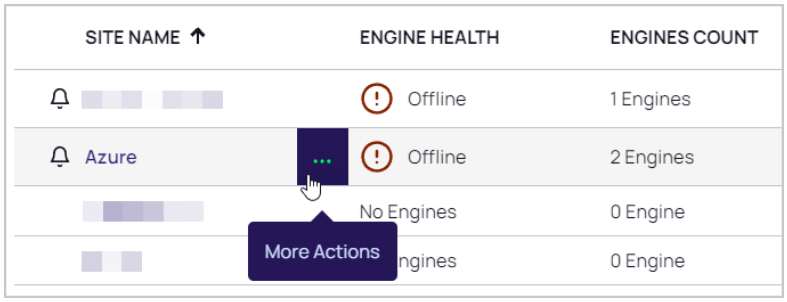
> **Important:** The SSH/RDP ports are set in the secret. Please review the Secret Server documentation for additional information. The RAS engine will use these ports to connect with the downstream targets.

Installing the Remote Access Engine

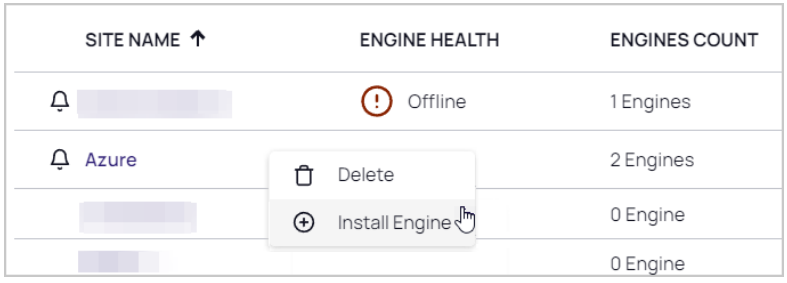
1. Log into the platform with administrative privileges.
2. From the left navigation menu, click **Settings**, then click **Remote access**.
3. On the Remote Access page, click the **Sites & Engines** tab.



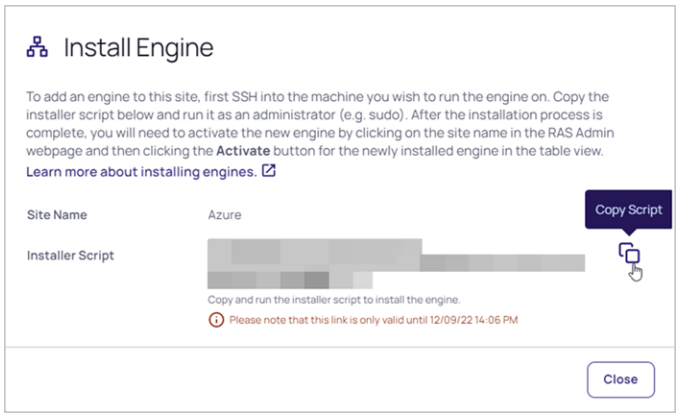
4. Hover your cursor in the site row, at the right side of the **Site Name** column.
5. Click the ellipses . . . that appears



6. From the pop-up click **Install Engine**.



7. On the **Install Engine** page, you can copy the entire installer script to you 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.



Installer 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 RAS 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 RAS Engine to Use a Proxy Server (Optional)

You can configure the RAS 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
```

3. Save and close the file.
4. You need to add the following `EnvironmentFile` attribute to the *Service* section of the RAS 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

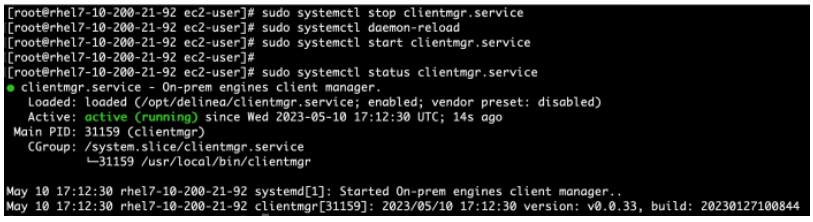
```
[Unit]
Description=On-prem engines client manager.
After=network.target
After=network.target

[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`

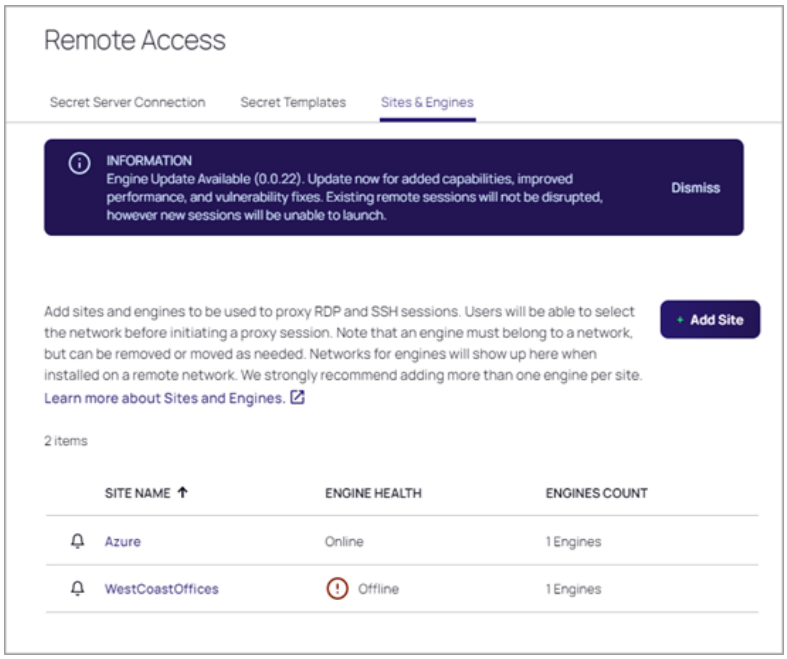
```
sudo systemctl stop clientmgr.service
sudo systemctl daemon-reload
sudo systemctl start clientmgr.service
```



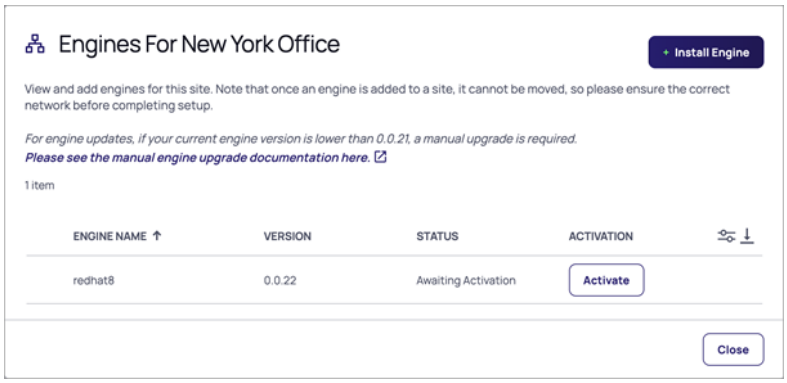
9. The system administrator may edit the environment file when necessary. After editing this file the system administrator will need to follow the steps above in step 6: *Restart clientmgr*.

Activate RAS Engines

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.



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.

Add Secret Templates to RAS

Secret Server Cloud

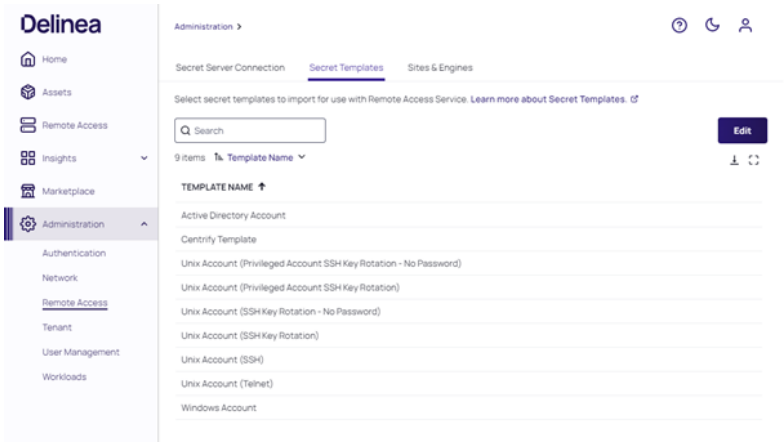
Secret Server Cloud customers entitled to Remote Access Service will automatically see the Remote Access launcher link on appropriate launchable secrets. Please refer to the Secret Server Integration documentation for more information on how to enable Secret Server in your Delinea Platform tenant.

Secret Server On Premises

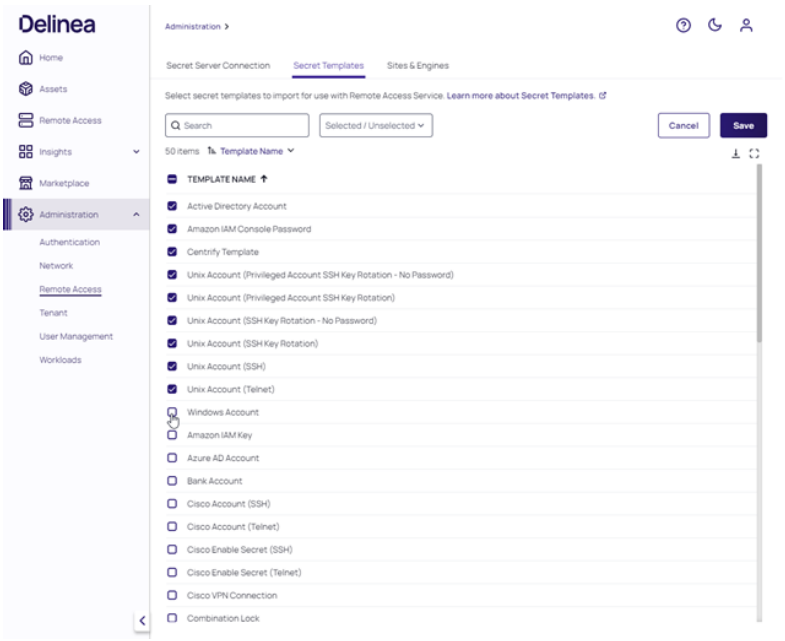
Before Secret Server On Premises customers can access RAS functionality on the Delinea Platform, administrators must enable one or more secret templates. Only secrets based on RAS-enabled secret templates will be displayed and available to users on the Remote Access page.

To enable templates for RAS, 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.



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.



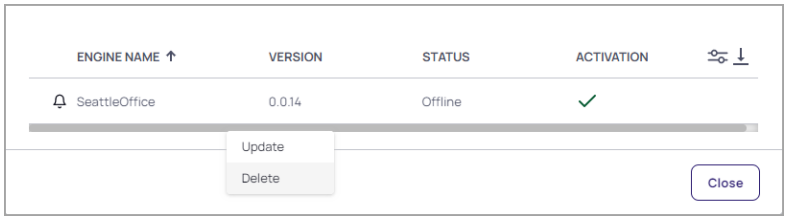
5. Click **Save** once you have added all of the needed templates.

Uninstall RAS Engines

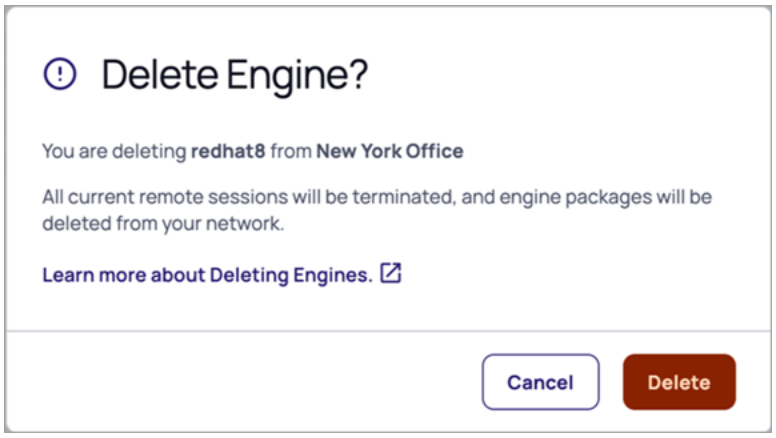
Automated Uninstallation

Note: This action removes the RAS engine from the portal and completely uninstalls the engine from your host.

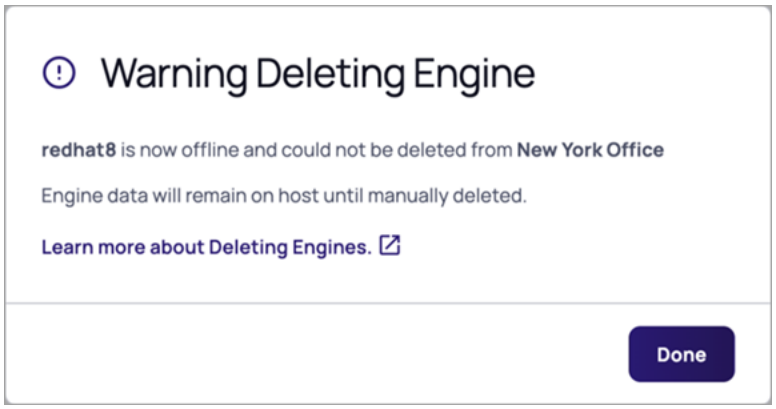
1. Log into the platform portal.
2. From the left navigation menu, click **Settings**, then click **Remote access**.
3. Click **Sites & Engines**.
4. Select the site.
5. On the Engine page, find the engine you want to delete and hover your mouse over that row.
6. Click the three dots that appear.
7. Click **Delete**.



You should see the following message.



If the above instructions do not completely uninstall the RAS 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 RAS engine server in question.
2. Run the following CLI command as a privileged user:

```
sudo /opt/delinea/updater -del
```

Using RAS

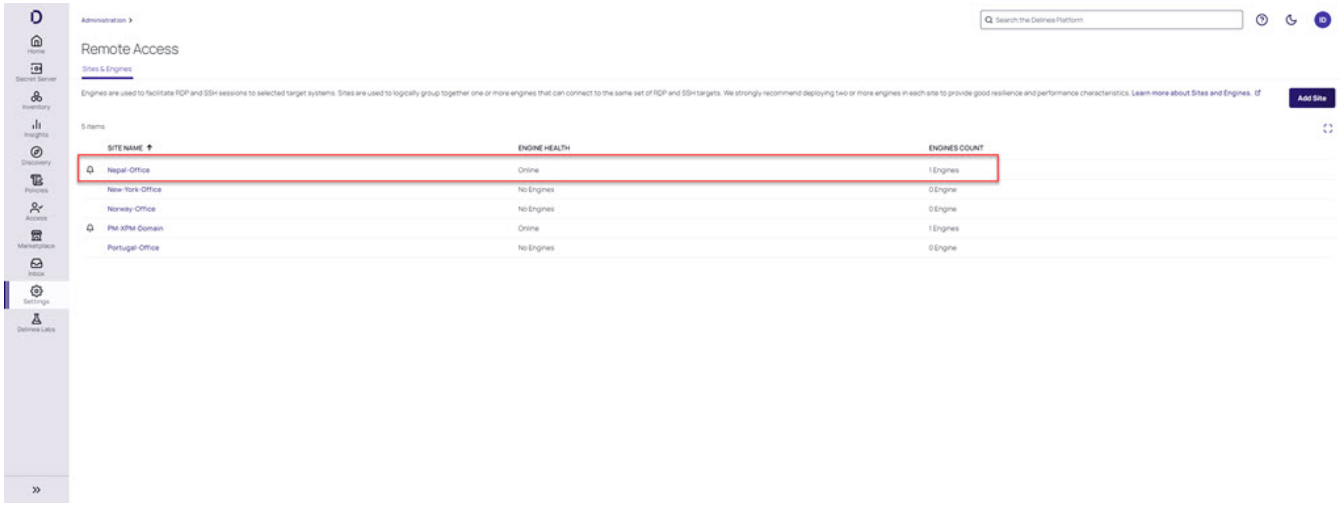
RAS Sites

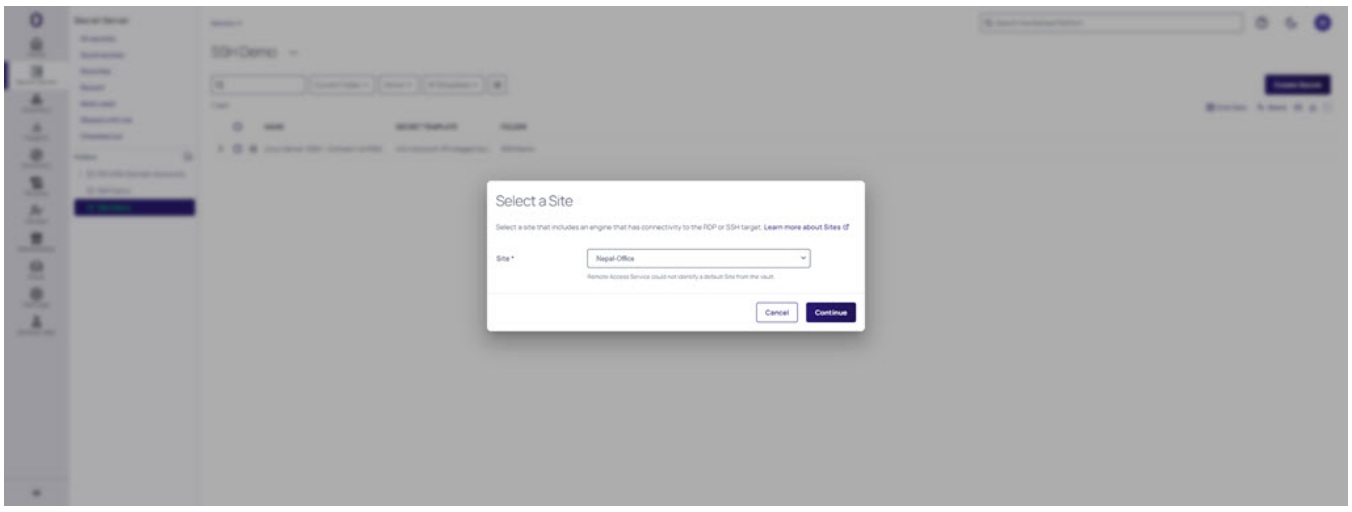
A RAS Site is the location where local (on-prem) Windows and Linux resources are stored. A Site includes the engines to which these resources are available. For reliability, it is recommended to add at least two engines to each site.

RAS 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 RAS Site

Delinea recommends that users name their RAS 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.





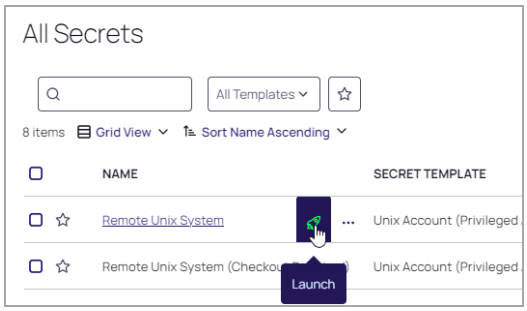
Note: The site selection drop-down is only prompted if the RAS Site name and the site used for the secret do not match.

Launch a RAS Session

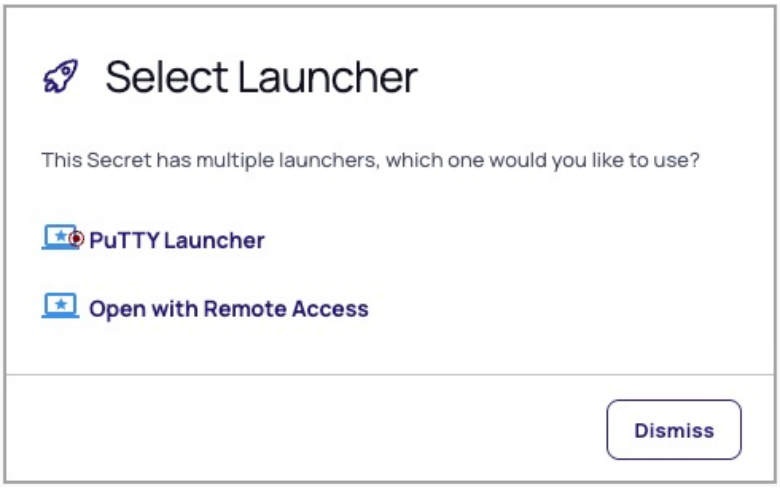
The Delinea Remote Access Service (RAS) runs entirely on the Delinea Platform interface, enabling users to quickly access and control remote computers.

To launch a RAS 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 RAS.
4. Hover your cursor over the Secret row
5. Click the rocket (launch) icon.



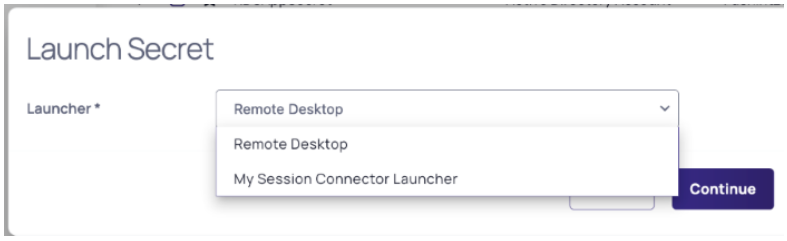
6. From the pop-up window, click **Open with Remote Access**.



7. From the pop-up window, select the appropriate site from the drop-down menu and click **Continue**.

Note: If a RAS Site name matches the vault Site name set on the Secret, the RAS Site is pre-selected in the Site Selection dialog. The site selection list is only shown when more than one RAS 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.

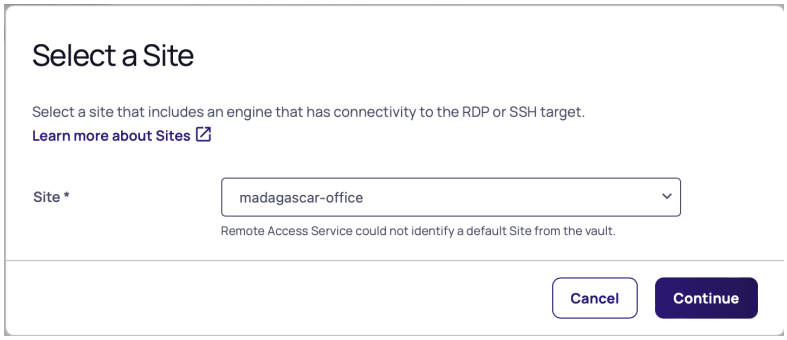


From Secret Server On Premises

This section describes how to launch secure RDP or SSH RAS 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 RAS Site name matches the Secret Server Site name set on the Secret, the RAS 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 RAS Engines

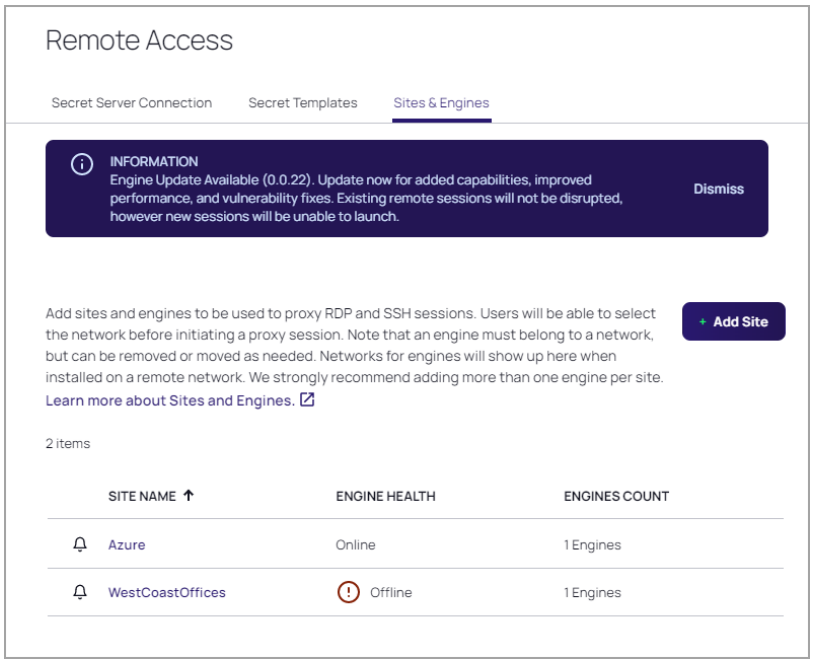
Delinea frequently releases new versions of the RAS on-prem engine. Administrators receive notifications through the platform UI that engine updates are available, as shown below. These notifications can be ignored with no negative consequences.

When a RAS 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 RAS 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 RAS Engine**, below). If your Delinea RAS engine is version 0.0.21 or higher, you can continue to the next section,**Updating a RAS Engine**.

Updating a RAS Engine

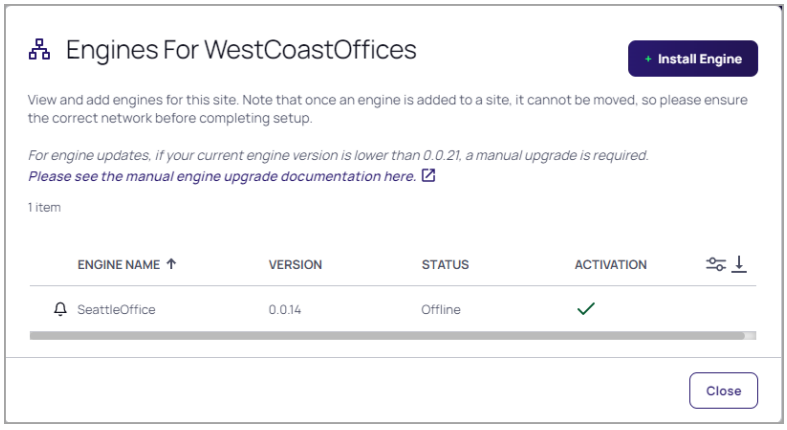
1. From the left navigation menu click **Settings**, then select **Remote access**
2. On the Sites & Engines tab, you can see the following:
   - The sites, listed under **Site Name**
   - The state of each site's engines under **Engine Health**
   - The number of engines on each site, under **Engines Count**.



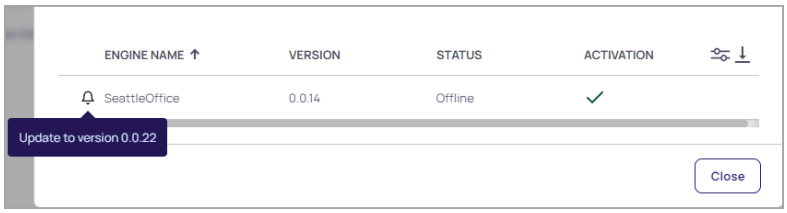
If one or more of your RAS engines is due for an update, you will see the following:

- 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!*

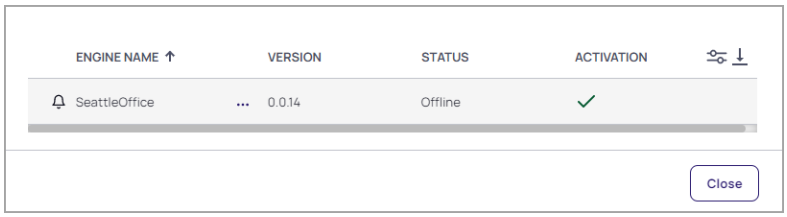
1. Click the name of the site where you wish to update an engine. The Engines page displays the engine's name, current version, status, and activation status.



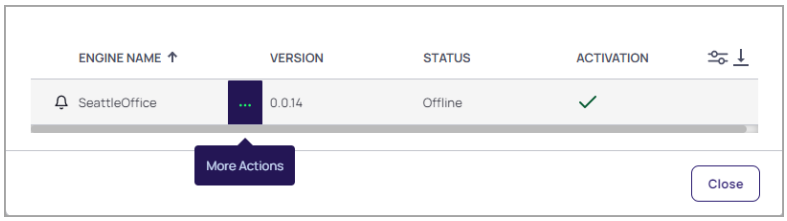
2. To see the version number of the newer engine you can upgrade to, hover your cursor over the bell icon.



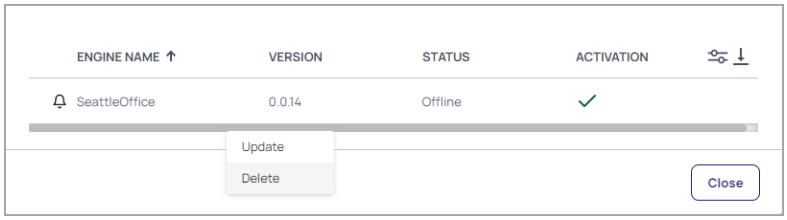
3. To update the engine, hover your cursor in the engine row. On the right side of the Engine Name column, three dots appear



4. Hover your cursor over the three dots. A pop-up appears saying *More Actions*.



5. Click the three dots and choose **Update**.



As the engine is updating, a daisy icon will appear in place of the bell. When a RAS 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 RAS Engine

To manually update a RAS 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 RAS on-prem engine.

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 RAS menu can be activated using Ctrl-Alt-Shift when keyboards need to be used for accessibility reasons. Users can tab though 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 "Transfer Files With RAS" on page 309.

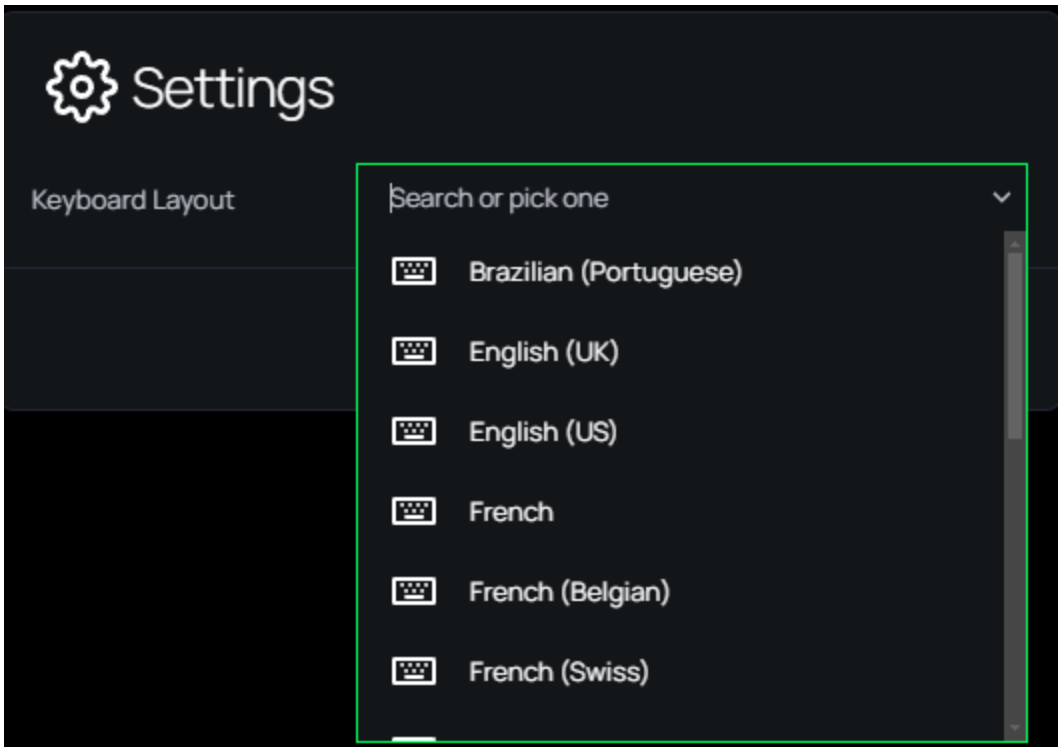
Session Information

Session Information allows users to get some quick information on their current RAS 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 RAS 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 RAS, 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.

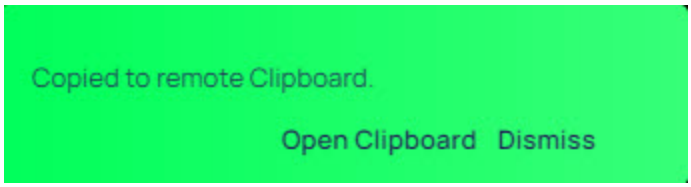
Screenshot

If a user clicks the **Take Screenshot** icon, RAS will automatically take a screenshot of the user's remote session and download the file to their local machine.

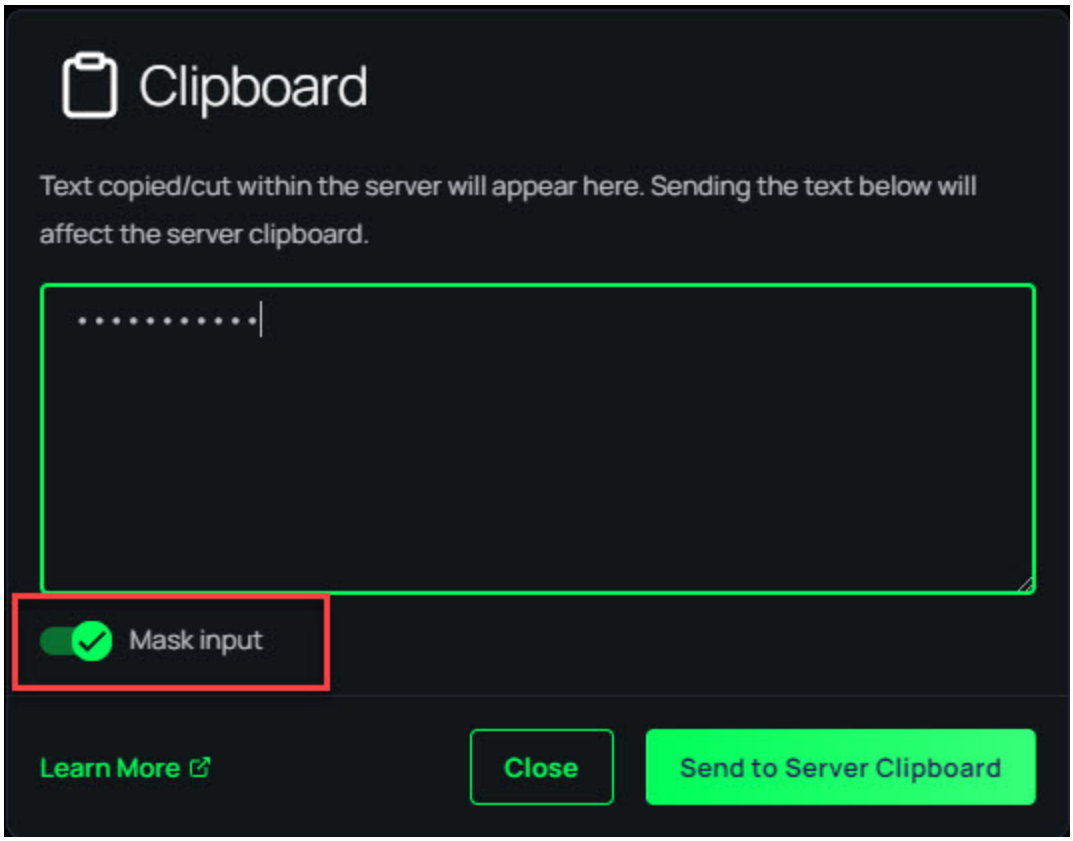
Clipboard

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. 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.

To copy from the remote target to your local machine, on SSH targets, simply highlight the needed text and this text will be automatically copied to the clipboard. For RDP targets, you will need to press *ctrl+c* or *right click > copy* after highlighting the text. Click **Open Clipboard** to view the copied text on your local machine.



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.



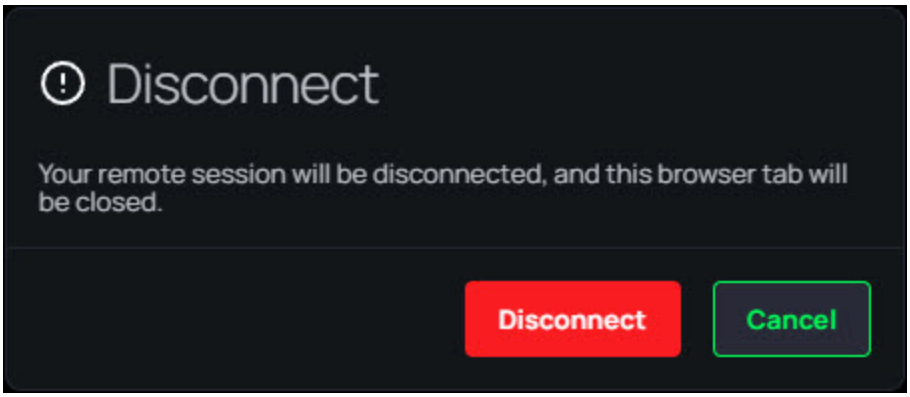
Note: RAS only supports unformatted text content with the clipboard.

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



.

Transfer Files With RAS

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, RAS will use SFTP.
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.

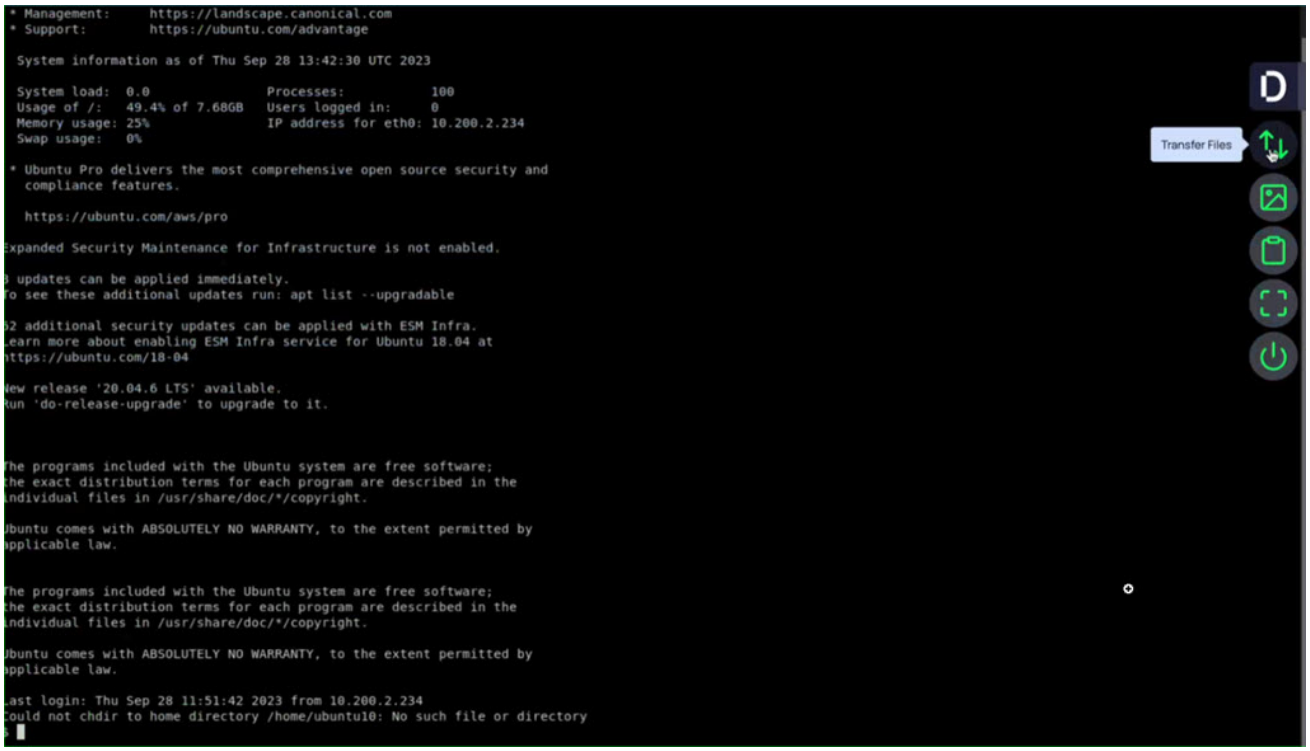
Administrators will need to ensure that users needing to upload or download files, are granted the following permissions:

- delinea.platform/remoteaccess/filetransfer/upload
- delinea.platform/remoteaccess/filetransfer/download

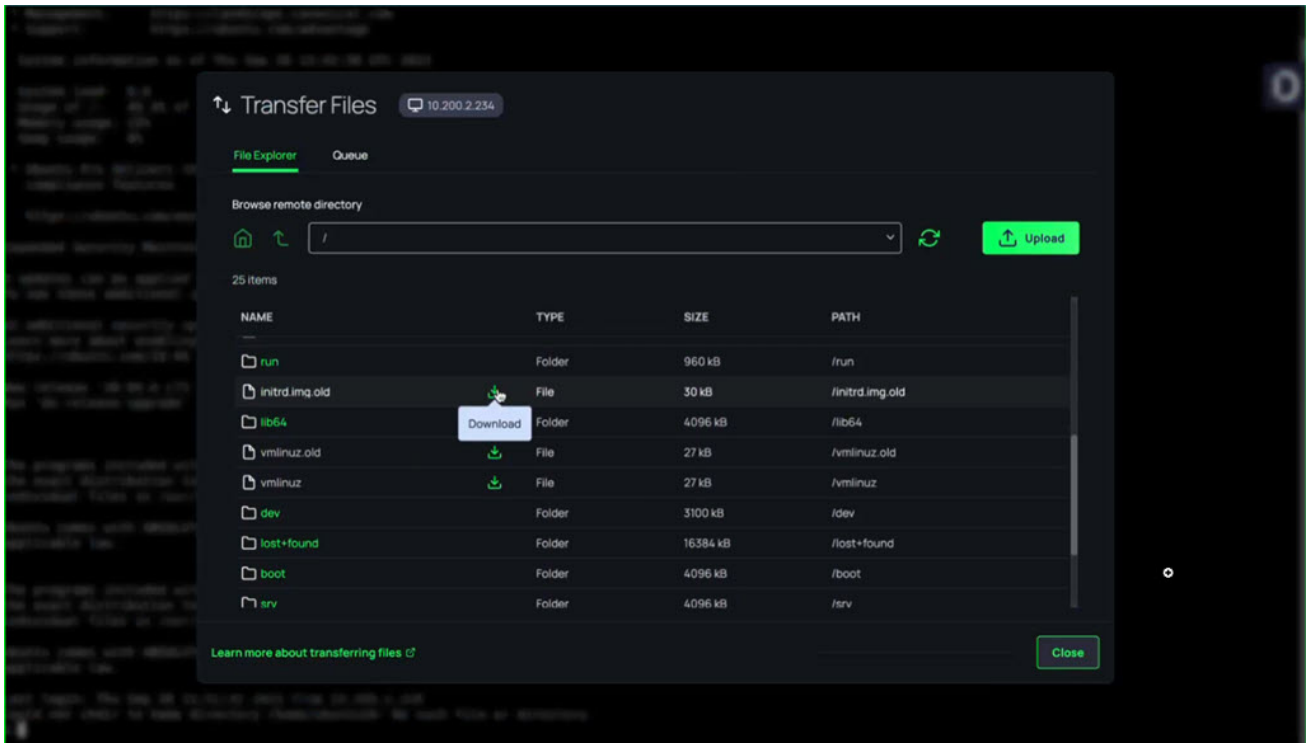
Please see "Remote Access Permissions and Roles" on page 315 for more information.

Download a File

1. Launch a RAS session to an SSH or RDP target. See Launch a RAS 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:



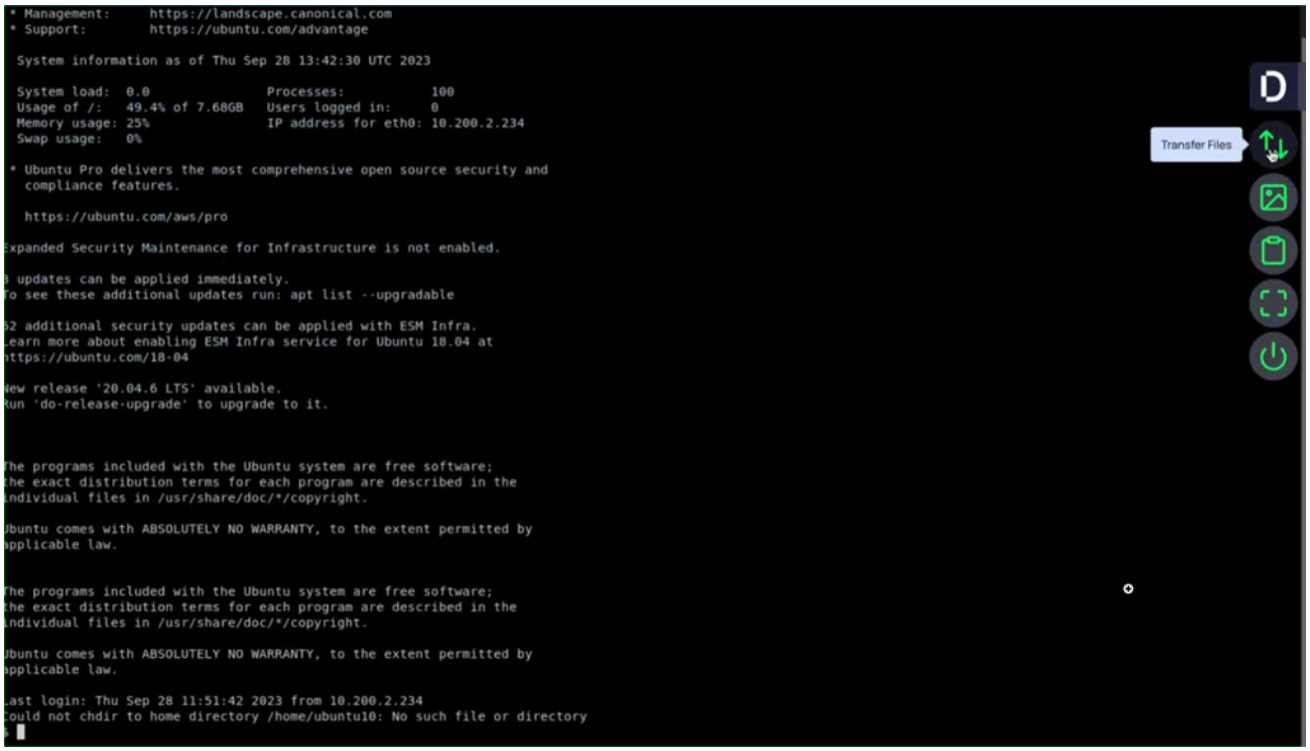
Users can close the file transfer window and continue to work with SSH/RDP connections while files are downloading in the background.

Note: If you do not see a download icon, you do not have the necessary permissions to download the file.

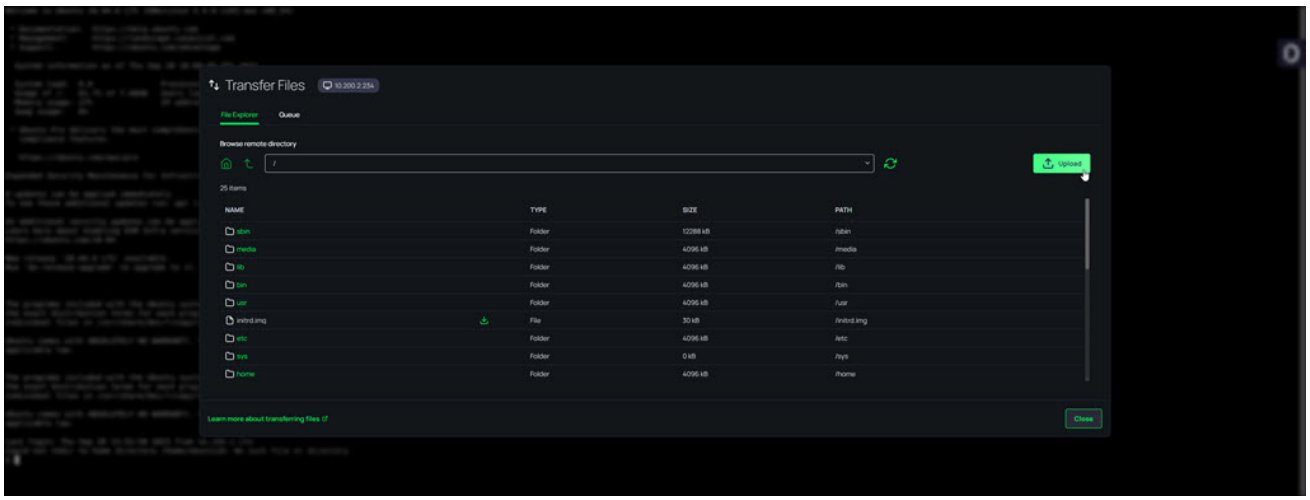
Upload Files

To upload files:

1. Launch a RAS session to an SSH or RDP target. See Launch a RAS Session for more information.
2. Click on the floating menu on right side and click **Transfer Files.**



3. Click the **Upload** button.



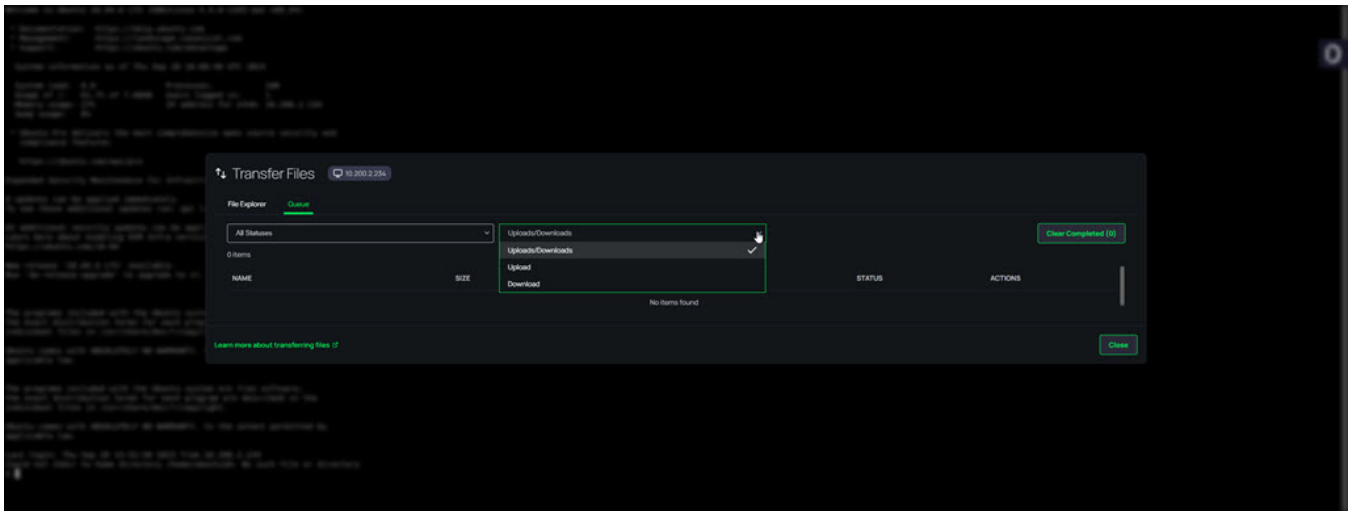
4. Users have the ability to select and enqueue multiple files for upload, with a limit of up to 500 files. Once enqueued, these files are displayed within the Queue tab for easy tracking. To maintain optimal performance, the system is configured to actively process up to 5 file uploads concurrently from the queue.

Users can close the file transfer window and continue to work with SSH/RDP connections while files are uploading in the background.

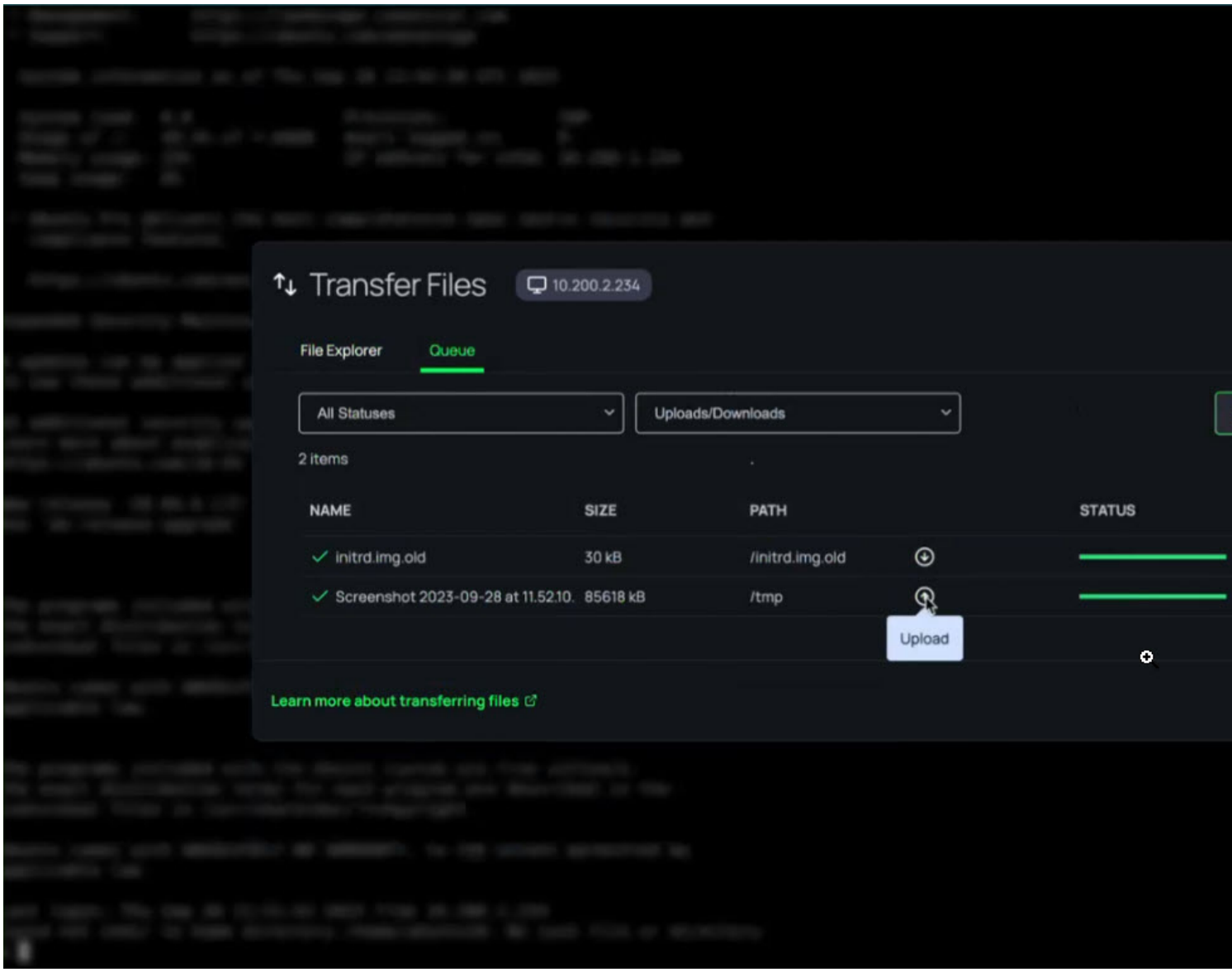
Note: If you do not see an **Upload** button, you do not have the necessary permissions to upload files.

Queue Tab

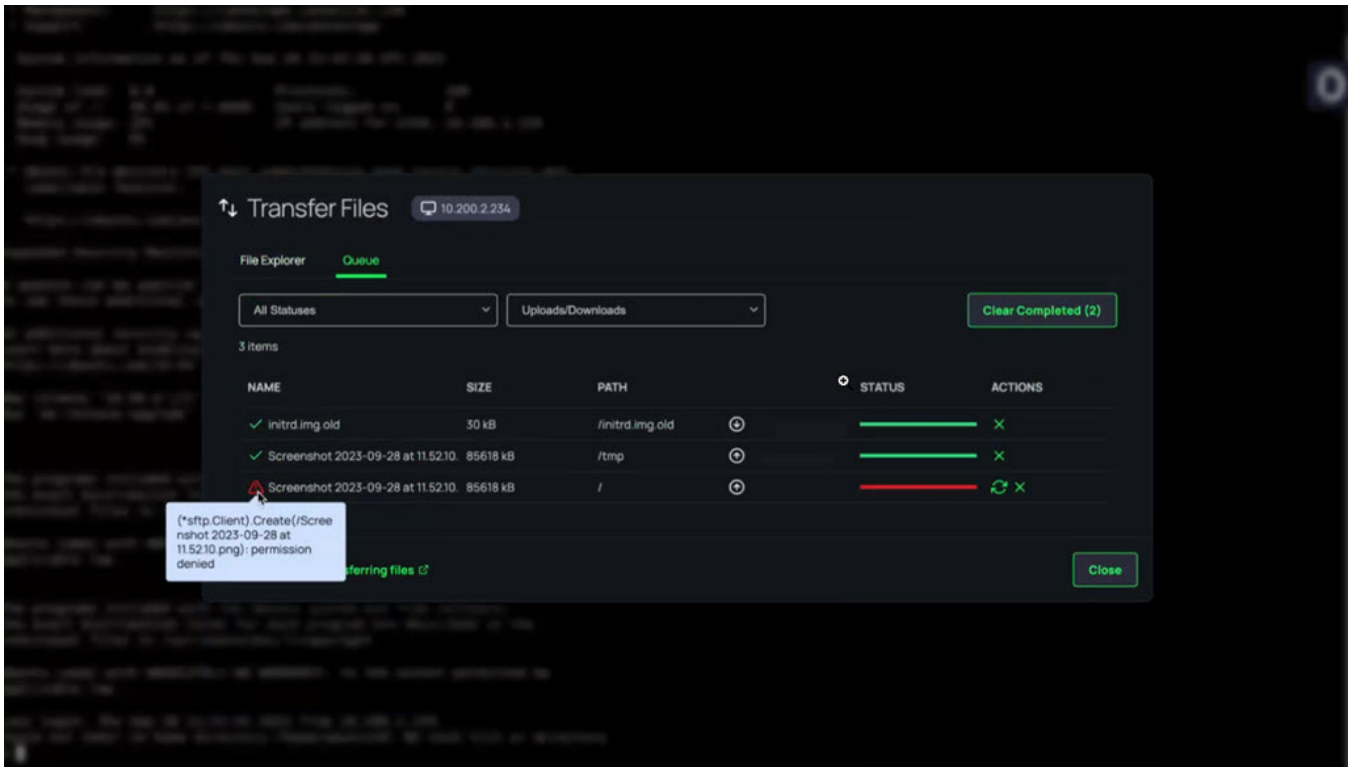
Inside the Queue tab, you can monitor the progress of your file uploads and downloads by selecting the desired view the drop-down menu:



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:

- RAS 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.
- The target system is enabled with *Use My Account*.
- 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.

Remote Access Permissions and Roles

The table below describes each permission available with RAS.

Permissions	Description	Permission List	RAS Users	RAS Admins
Launch RAS Session	Launch a remote session. *Needed to use RAS.*	delinea.platform/remoteaccess/session/launch	Yes	Yes
View Secrets	View the secrets in the Remote Access page. Applicable only for On-Prem Secret Server customers. *Needed to use RAS.*	delinea.platform/remoteaccess/secret/read	Yes	Yes
View RAS Engine	View the UI of a Remote Access engine.	delinea.platform/administration/remoteaccess/engine/read	N/A	Yes
Activate RAS Engine	Activate an engine to access and connect to your remote systems through a site and engine	delinea.platform/administration/remoteaccess/engine/activate	N/A	Yes

Permissions	Description	Permission List	RAS Users	RAS Admins
Add RAS Engine	Add an additional Remote Access engine to connect to remote systems.	delinea.platform/administration/remoteaccess/engine/create	N/A	Yes
Delete RAS Engine	Remove a Remote Access Engine from the server via automated uninstall or manually.	delinea.platform/administration/remoteaccess/engine/delete	N/A	Yes
Update RAS Engine	Deploy the latest updates to your Remote Access engines.	delinea.platform/administration/remoteaccess/engine/update	N/A	Yes
Create RAS Site	Create a new Remote Access site.	delinea.platform/administration/remoteaccess/site/create	N/A	Yes
Delete RAS Site	Remove a Remote Access site.	delinea.platform/administration/remoteaccess/site/delete	N/A	Yes
View RAS Site	View Remote Access site details.	delinea.platform/administration/remoteaccess/site/read	N/A	Yes
Update RAS Site	Rename a Remote Access Site.	delinea.platform/administration/remoteaccess/site/update	N/A	Yes

Permissions	Description	Permission List	RAS Users	RAS Admins
Upload Files	Upload files from a local machine to a remote target.	delinea.platform/remoteaccess/filetransfer/upload	N/A	Yes
Download Files	Download files from remote target to a local machine	delinea.platform/remoteaccess/filetransfer/download	N/A	Yes
Create Secret Server Templates	Enable a Secret Server template. Only secrets based on Remote Access-enabled secret templates will be displayed and available to users on the Remote Access page. *Only applicable for Secret Server On Premises.*	delinea.platform/administration/remoteaccess/secrettemplate/create	N/A	Yes

Permissions	Description	Permission List	RAS Users	RAS Admins
Delete Secret Server Templates	Remove a secret template. *Only applicable for Secret Server On Premises.*	delinea.platform/administration/remoteaccess/secrettemplate/delete	N/A	Yes
View Secret Server Templates	View the UI of the secret template. *Only applicable for Secret Server On Premises.*	delinea.platform/administration/remoteaccess/secrettemplate/read	N/A	Yes
Configure Secret Server Connection	Configure Remote Access Site for Secret Server Connection. *Only applicable for Secret Server On Premises.*	delinea.platform/administration/remoteaccess/vault/configure	N/A	Yes
View RAS Vault	View the 'Secret Server Connection' UI. *Only applicable for Secret Server On Premises.*	delinea.platform/administration/remoteaccess/vault/read	N/A	Yes

RAS Engine Host Hardening

This topic discusses best practices for hardening Remote Service Access (RAS) engine servers.

RAS engines do not store any passwords, PII, or user data in any configuration files.

General Hardening Steps

Restrict Incoming Port Access to All RAS Engine Servers

RAS 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 RAS 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)

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.

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:

- 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

The following are Delinea recommended best practices for hardening the Ubuntu Linux distribution running the RAS 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.

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)

The following are Delinea recommended best practices for hardening the RHEL distribution running the RAS 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).

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.

Entitlements and Licenses

RAS concurrent user licenses entitle users on that tenant to connect to remote systems using RAS. 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 RAS 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 "Managing Third-Party Contractors and Vendors" on page 417.

Please note that RAS 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.

RAS Troubleshooting

This section provides helpful troubleshooting tips and answers to frequently asked questions.

- Connecting to Target Issues
- Failed to Connect to the Target Machine
- Installation Issues
- Engine Server Issues
- Start/Stop Commands
- Distributed Engine Issues

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

RAS 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.

Other Encryption/Authentication modes are NOT currently supported.

- Standard RDP Security
- Kerberos authentication

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:
   - RAS 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 Target 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.

- 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.

The Engine Shows as "Offline" in the Sites and Engines 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/snapd/snap/snapd/17883
/dev/loop1       64M   64M     0 100% /var/lib/snapd/snap/core20/1695
/dev/loop2      6.7M  6.7M     0 100% /var/lib/snapd/snap/links/60
/dev/loop3       64M   64M     0 100% /var/lib/snapd/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 in Skytap

Before creating a static UUID, check to see if the engine is offline by running the following command:

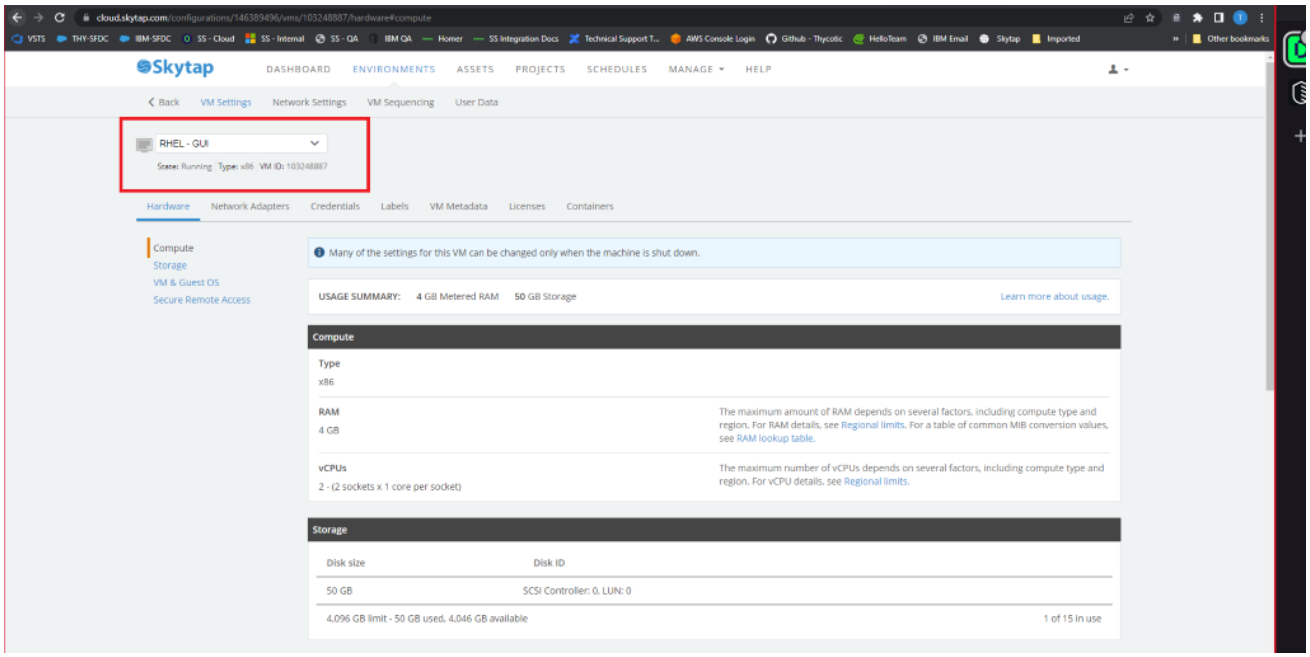
```
sudo systemctl status clientmgr.service
```

If the web UI shows the engine is offline, proceed to creating a static UUID:

1. SSH into the server with the following command:

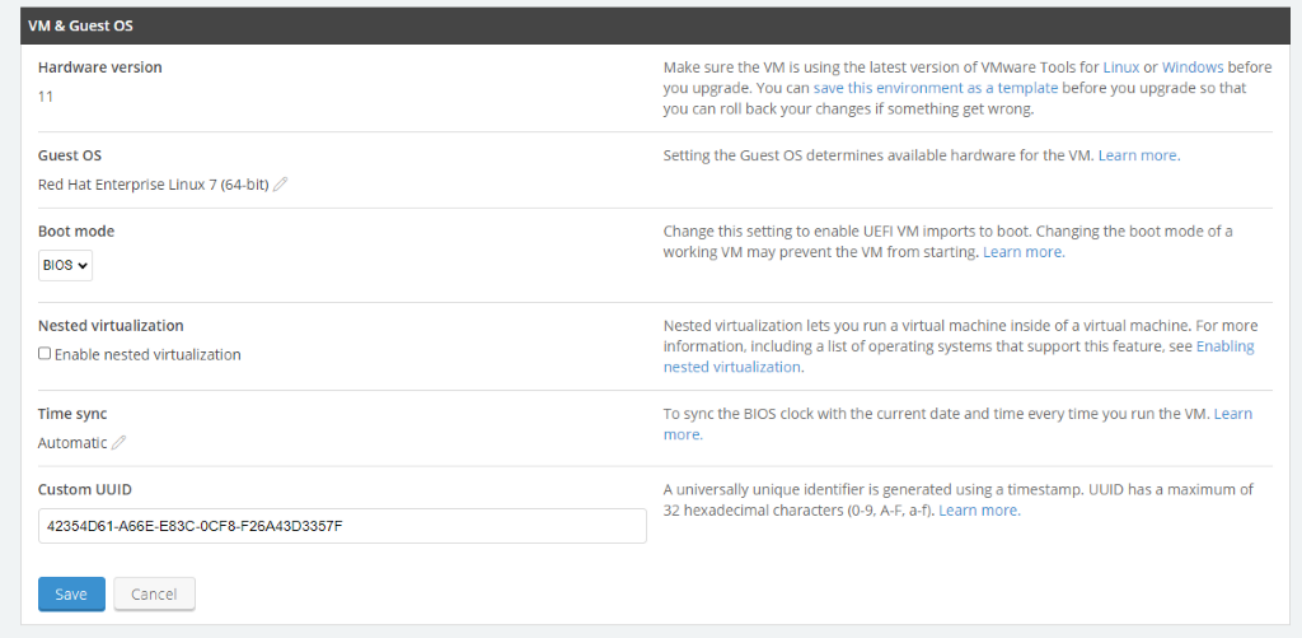
   ```
   sudo cat /sys/devices/virtual/dmi/id/product_uuid
   ```

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.



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 RAS engine

Issues Encountered While Installing the RAS Engine

If users encounter issues during RAS 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

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 RAS."
   - **Solution:** User must have root access to run the installer
2. A previously installed version of the RAS engine has been detected
   - **Error msg:** "A previously installed version of RAS has been detected."
   - **Solution:** User must un-install the currently installed RAS 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 RAS 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 RAS engine. Please install the RAS 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 RAS 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 RAS Engine is Not Working From the Web UI.

1. SSH into the server hosting the RAS engine
2. Run the following CLI command as a privileged user:

```
- sudo /opt/delinea/updater -del
```

3. To uninstall RAS engines from the Web UI, see Uninstall RAS Engines.

Start/Stop Commands

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 RAS engine:

  ```
  sudo systemctl stop clientmgr.service; echo $?
  ```

- To manually start the RAS engine:

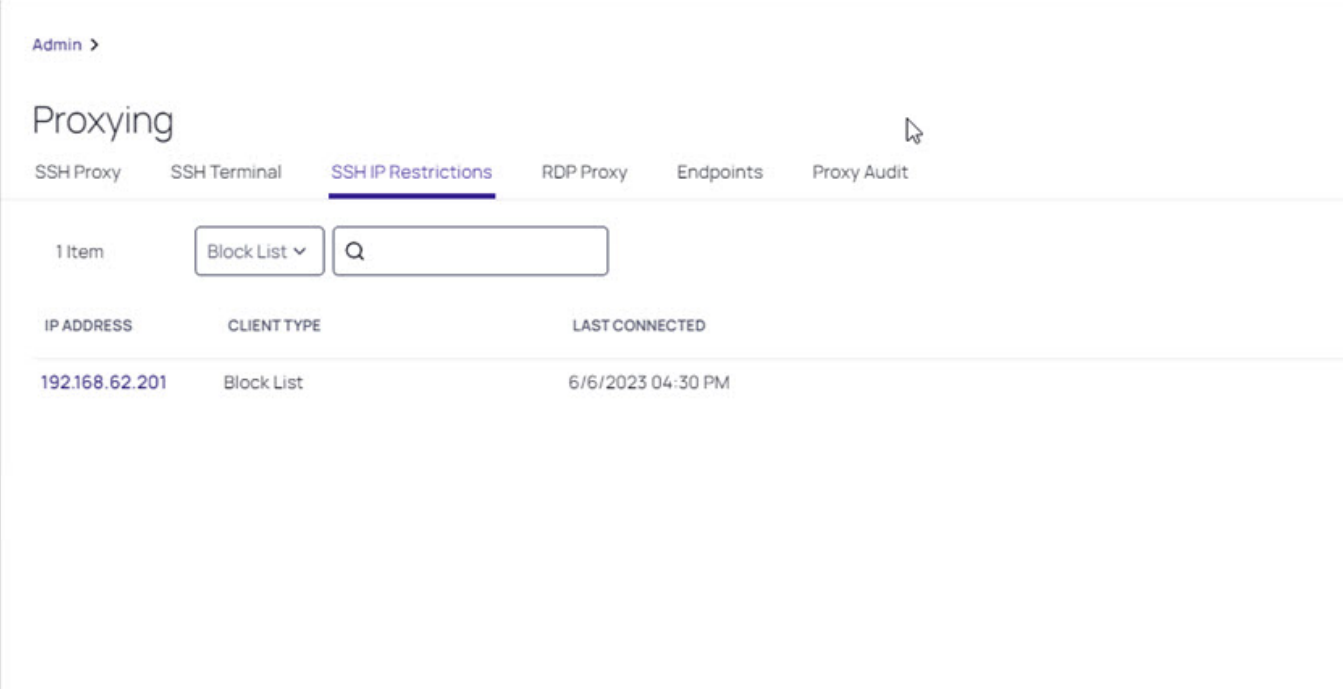
```
sudo systemctl start clientmgr.service; echo $?
```

Note: Look for the 0 to verify that the commands were successful. Any other value indicates a failure

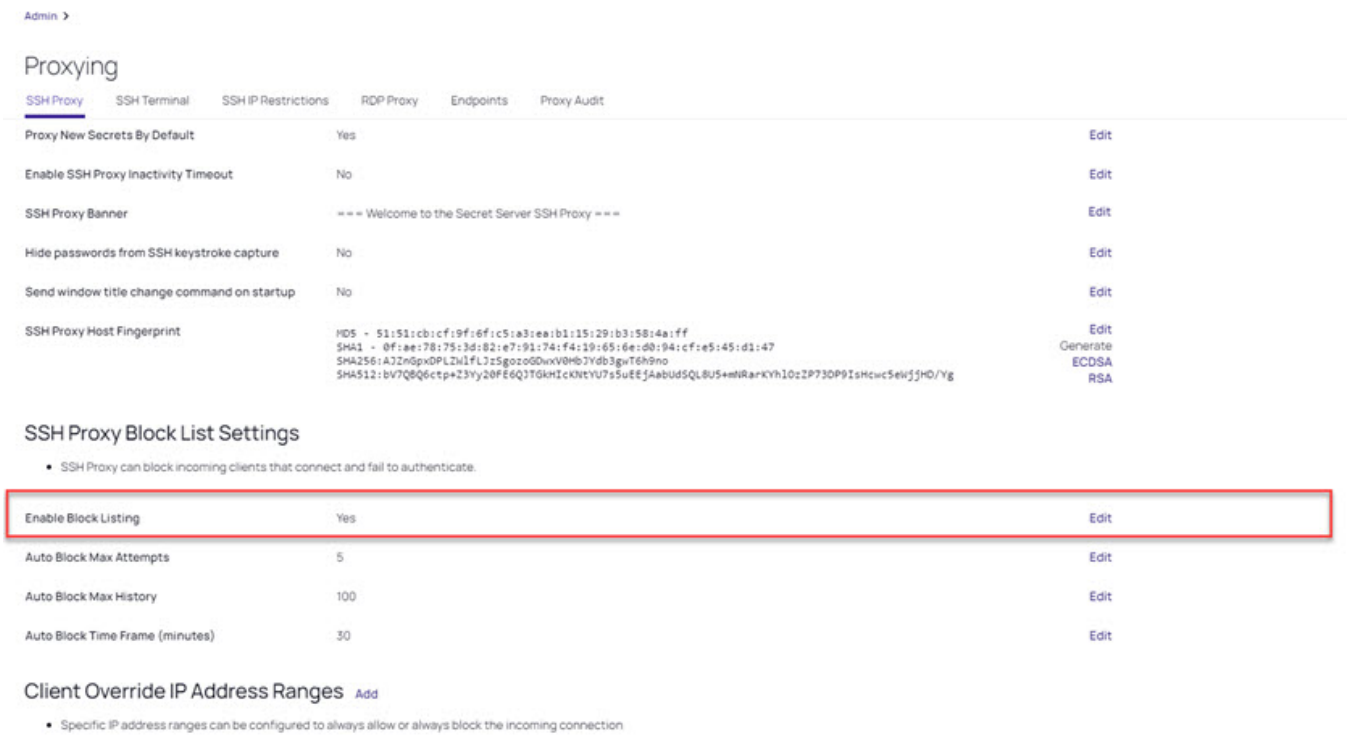
Unable to Launch SSH Sessions via Secret Server Distributed Engine

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.
3. 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.



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 RAS engine cannot connect to the target on-prem Secret Server, check if the on-prem Secret Server is accessible from the RAS engine by running the following commands:

```
curl -kv https://ON PREM SECRET SERVER DOMAIN NAME or IP ADDRESS/api/v1/users/current
```

Insights

Delinea Insights provides the core services for security and analytics. It is composed of two essential services: Audit and Behavioral Analytics.

Audit

This service meticulously logs activities of users and services, serving as a reliable source for auditing. It ensures accountability and provides a comprehensive record that can be used for in-depth analysis.

Behavioral Analytics

The data captured by our auditing service is further enriched through Delinea's behavioral analytics. By employing advanced deep learning algorithms and scrutinizing historical user behavior data, we can identify and flag risky actions with precision.

Our integration of these services allows for the delivery of real-time alerts, substantially reducing the risk of potential damage and enhancing the security posture of your enterprise.

Audit

The Delinea Platform auditing features include:

- "Viewing Audit Logs" on page 344
- "Reviewing Sessions" below

Reviewing Sessions

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.

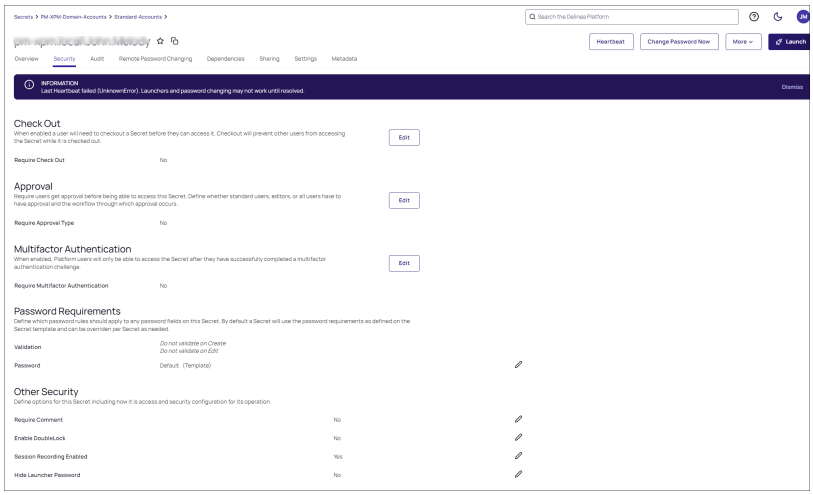
Session Review allows administrators with the appropriate permission to view all active launched sessions within the platform. If Session Review is enabled on the secret, an administrator can watch the user's session in real time or once the session recording has been completed.

Enabling Session Review

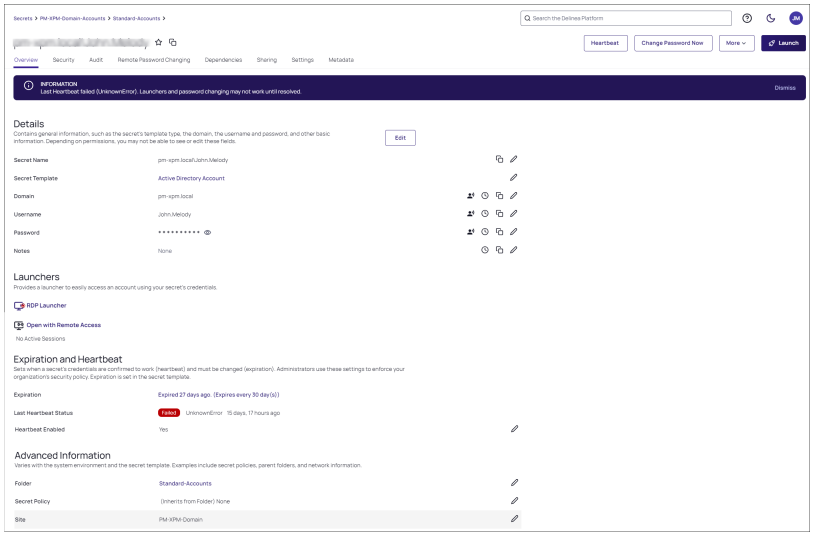
You can view session recordings on the platform once a session recording has been configured within the vault on both the tenant and secret level. Refer to Configuring Session Recording to configure Session Recordings within your Secret Server Cloud instance.

Launching a RAS Session with Session Review Enabled

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



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



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, which in turn requires an 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.

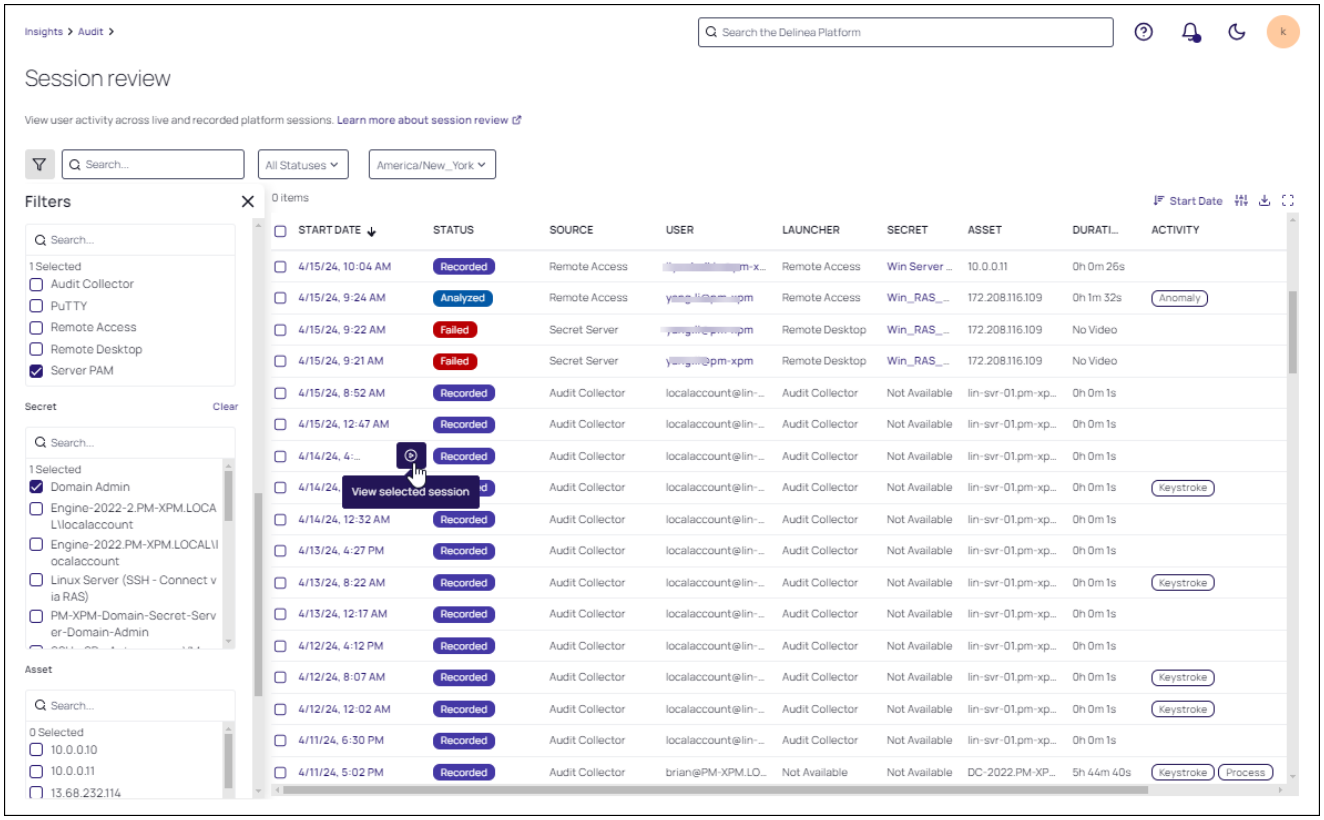
SSH keystroke data relies on the Secret Server SSH Proxy. This can be enabled under Admin > SSH Proxy. See SSH Proxy Configuration.

Once the proxy is enabled, recorded SSH sessions will log SSH traffic which can be searched and displayed in the Session Recording playback interface. See "Viewing Sessions" below.

Viewing Sessions

When first accessed, the Session Review page lists each session you have access to (Delinea Platform and other native sessions).

Hover over an entry to enable a view icon ⊙. Click the icon to view the session. You can select a group of sessions (two or more) to review by selecting the check box for each session.



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

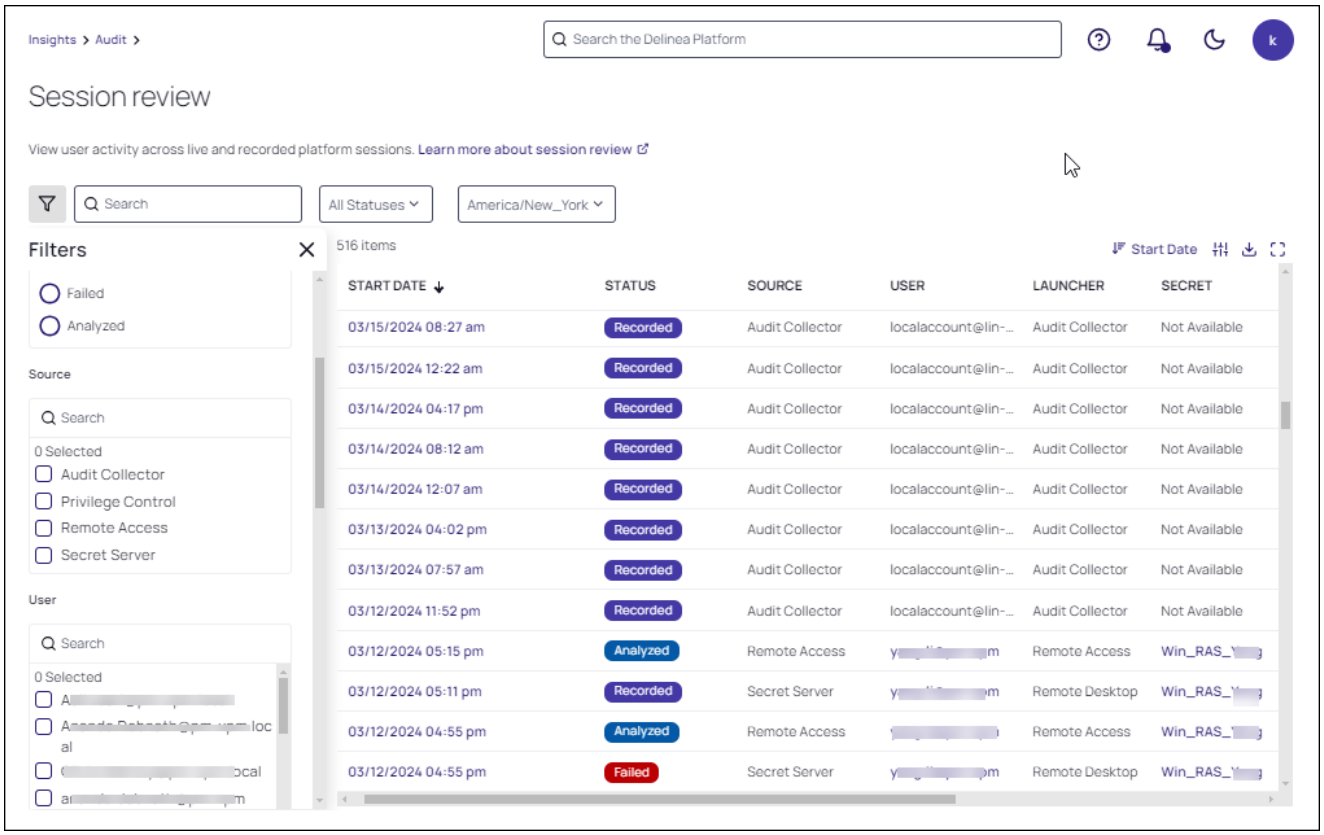
Activity	Any activity detected in the session. Categories include: **Anomaly** - activity that deviates from the norm **Keystroke** - client keystroke activity **Process** - application executions on the endpoint
Start Date	The time and date when the remote session was initiated.
Sesson ID	The unique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

Status	Session recordings go through the following lifecycle. **Live**: This is an active session. You can view a live stream of the remote session in near real time **Recorded**: Once encoding the session is successfully completed, the final recording is available to review. **Finished**: The session was completed, but session recording was not enabled for viewing. **Failed**: Any session that has not completed recording or encoding. **Analyzed**: The video was transcribed and analyzed by Delinea AI to detect risk. Note: Use the **All Statuses** pull-down to limit the display of recording to a particular status.
Source	Represents the service from which the remote session was launched.
User	The username who launched the remote session. Click an available USER link to view that user's "Managing Users" on page 192.
Launcher	The various methods or triggers used to initiate session recordings.
Secret	The vaulted secret used to launch the remote session. Users are able to drill down into the secret directly to view additional details about the secret, assuming proper permissions exist. Click an available SECRET link to view its secret key information on Secret Server.
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 Platform.
Duration	The total time recorded for the session.

Searching and Filtering Sessions

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

You can also select the filter icon on the left of the search box to further specify the criteria. You can filter by **Status**, as well as specific data in any of the displayed columns.

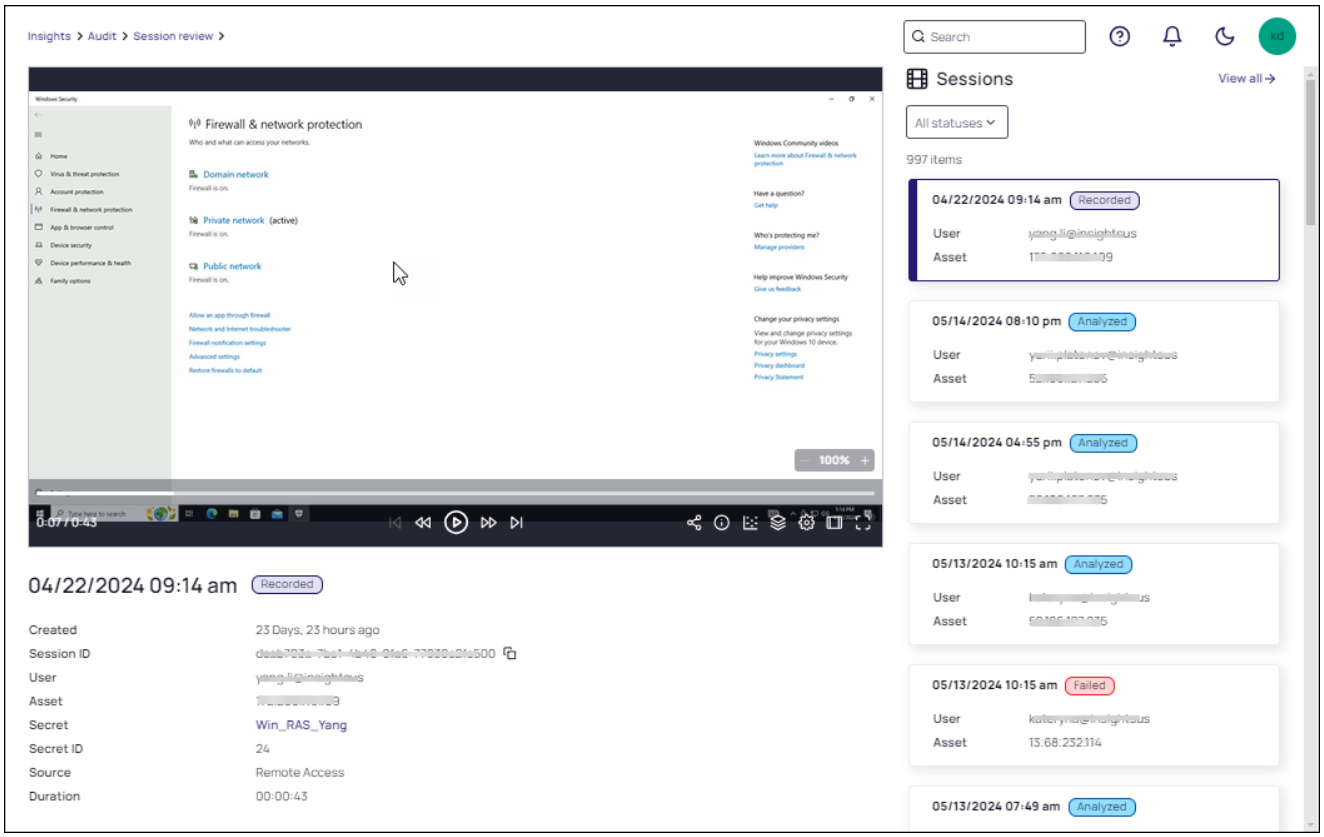


Navigating the Video Player and Session Review Panel

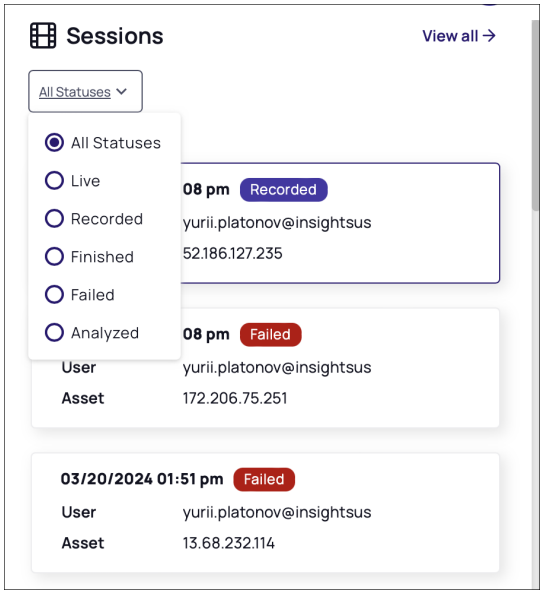
Once you select a session or a group of sessions with recordings, you will be redirected to view the recording in the video player. Click any card in the Sessions Review panel to view the associated recording in the video player.

Refer to "Using Video Features" on page 342 for video playback controls and analysis features. Information fields are displayed directly under the player.

In addition to the fields displayed in the Session Review table, the time since the video was recorded is displayed.



Filter the display of various statuses of recordings in the panel using the **All Statuses** pull-down.



Using Video Features

Video Playback

Playback controls include the following.

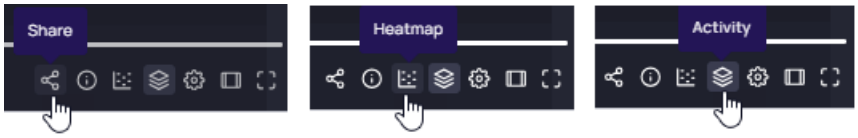
- Full Screen: Display video on your entire window
- Theatre Mode: Enables/disables the display of theatre viewing mode
- Play/Pause: Play or pause the session
- Previous/Next: Navigate to the previous or next session recording
- Forward/Rewind: Jump or rewind the recording at 10 second intervals

Click the Settings icon in the video tray for Speed controls. To zoom 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 Features

In addition to the video playback controls, Session Review includes the following features.

- Activity enables/disables the Activity panel. In the panel, **Analysis with Delinea AI** will produce a transcript of activity, along with any anomalies identified. Refer to "Analyzing a Recording" below
- The Heatmap feature enables/disables the display of a color-coded view of activity. Refer to "Analyzing a Recording" below.
- Session Sharing allows you to send a link to a video to other users on the platform. Refer to "Sharing Sessions" on page 344.



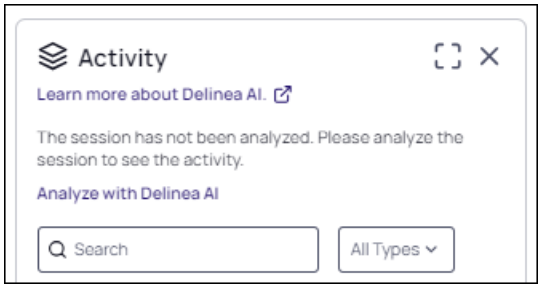
Analyzing a Recording

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

Session Recording allows you to transcribe the activity in the video for further analysis and also display activity as a heatmap,

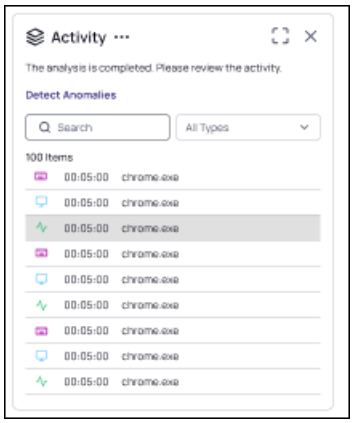
Viewing Activity

Select a recorded session and click the **Analyze with Delinea AI** link in the Activity panel.



When analysis is complete, the recording is labeled **Analyze** and the following features are available:

- Enable **Autoscroll** to automatically sync the video player with the selected activity item. Click either the activity in the Activity Panel or a time in the player's time line to sync.
- Click **Detect Anomalies** to enable viewing of activity anomalies. Each anomaly in the transcript displays the transcribed text, followed by an Open AI description of the anomaly.
- Use the **Type** pull-down to switch the transcript between **All Activities**, **OCR**, and **Anomaly** view.
- **Clear Transcript** is available in the Activity pull-down to clear the transcription and its related anomaly data from the session.



Viewing the Heatmap

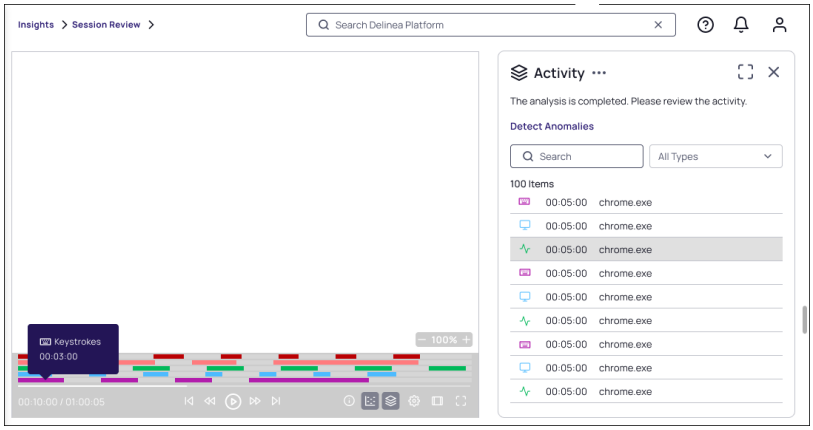
After a video is analyzed, click the Heatmap icon in the video tray to access a heatmap of the current session. See "Using Video Features" on the previous page.

The colors displayed in the heatmap correspond to types of activities indicated by the Activity Heatmap key (information icon). These include:

- Red - anomaly
- Purple - keystroke
- Green - process

- Blue - screen
- Orange - OCR

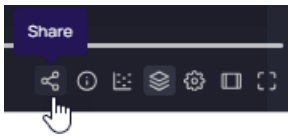
The intensity of color on the heatmap relates directly to the intensity of activity across time. Click a specific interval on the heatmap to update the transcript to reflect that activity. Hover over an area of activity to view details.



Sharing Sessions

You can share recordings within the platform with other users, as long as the same session recording permissions exist between those users. Refer to "Roles and Permissions" on page 217.

1. At the Session review page, select the recording you want to share.
2. In the video player controls, click the Share icon.



3. At the Share a link dialog, click the copy icon. Share the URL produced via your preferred method (e.g., email, messenger, etc.).

   Note: Prior to clicking Share, you can select a specific time in the video to begin the share.

Viewing Audit Logs

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

Accessing Audit Logs

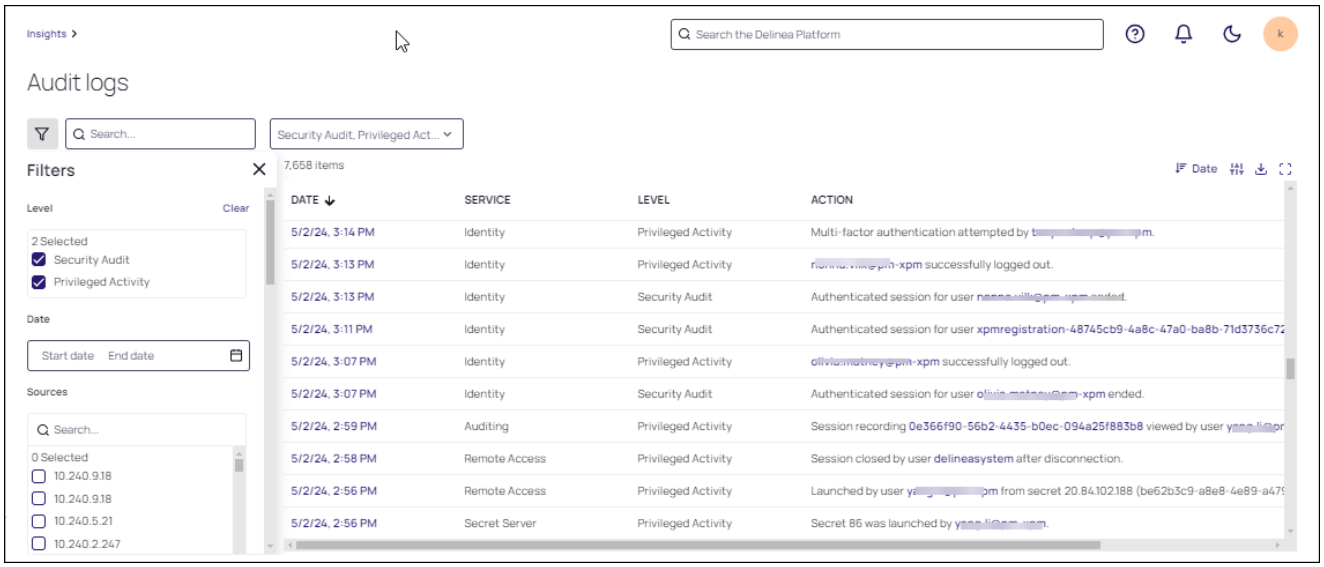
To access Audit logs, follow these steps:

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



Customizing the Table

The table columns present data types associated with the event. Some columns are sortable in either ascending or descending order. The columns presented are also customizable using the Displayed Columns icon.

These data types are:

- **Date**: the date the event occurred
- **Service**: The application that is monitored and presented in the Audit logs. Refer to Service Levels for a description of the services available for monitoring.
- **Level**: The functionality (in a Service) that is monitored. Refer to Service Levels for a description of the levels available for monitoring.
- **Action**: the action that produced the event
- **Initiated By**: the name of the user initiated the event
- **Target**: The platform component involved in the event
- **Source**: the source of the event, such as RAS, Web Password Filler, or Secret Launcher

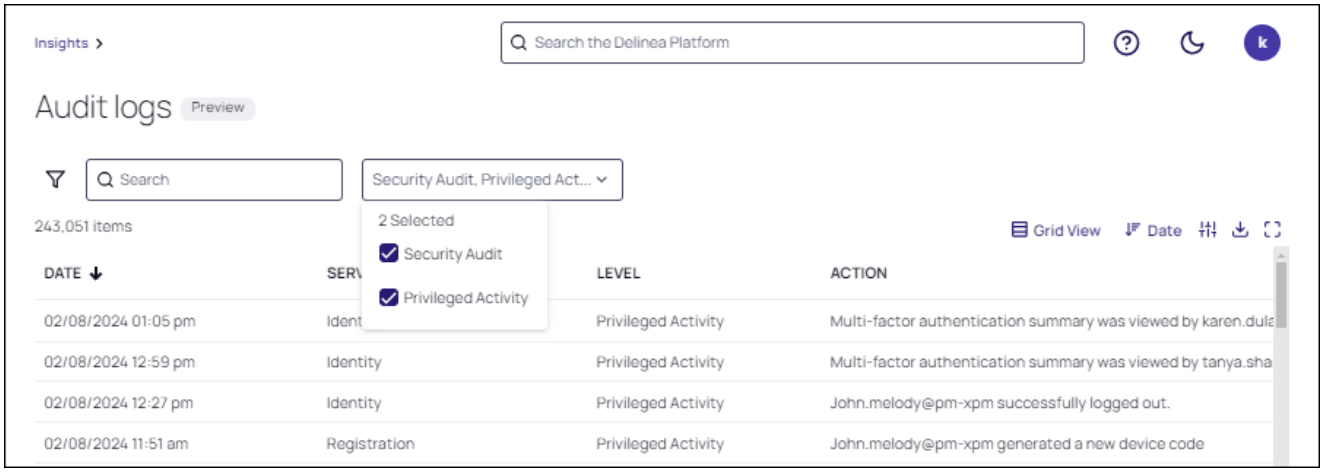
Filtering Events

Click the Filter icon. The Events presented in the table can be dynamically filtered according to the following criteria that you define in the left Filter panel.

Selecting Audit Levels for Display

Auditing serves as a collector for event logs. These logs are differentiated into the following three categories, selectable at the **Level** pull-down.

- **Security Audit** logs are critical actions such as configuration change in Delinea services.
- **Privileged Activity** logs are important actions such as creating secrets, viewing passwords, launching elevated process on an endpoint.



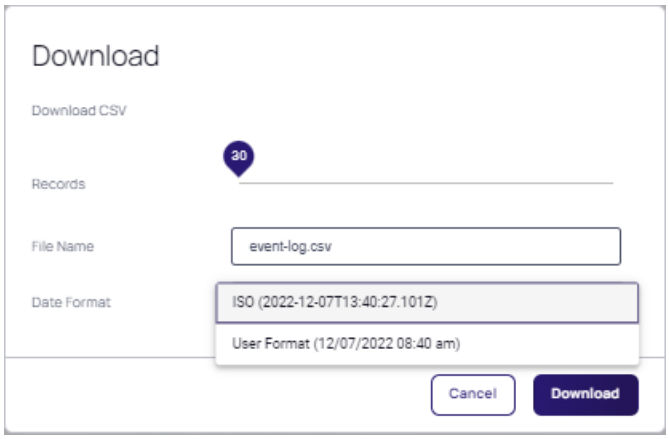
For a detailed list of the Services that support these levels, refer to the following:

- "Secret Server Services" on the next page
- "Permissions Services" on page 368
- "Registration Services" on page 373
- "Identity Services" on page 370
- "RAS Services" on page 372
- "Audit Collector Services" on page 354
- "Certificate Management Services" on page 370

Downloading Data

The data from the event log can be downloaded as a CSV file, in either a **User Format** or **ISO** format as the format for the CSV file label.

Click the Download icon in the top control bar. At the Download dialog, specify a **File Name** and **Data Format**, then click **Download**.



Secret Server Services

The Secret Server service monitors events related to Secret Server for any activity related to the 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.
- 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}}.
- 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}}.
- 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}}.
- 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}}.
- 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}}.
- 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.

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}}.
- 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}}.
- 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 Centrify Identity Services Platform failed for user {{Actor.Name}}.
- Disabling Centrify Identity Services Platform failed for user {{Actor.Name}}.
- Local user was enabled by user {{Actor.Name}}.
- Centrify Identity Services Platform was successfully enabled by user {{Actor.Name}}.
- Local user was disabled by user {{Actor.Name}}.
- Centrify 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}}.
- 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}}.

Insights

- 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}}.
- 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}}.
- 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}}.
- 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}}.
- 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}}.
- 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}}.
- 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}}.
- 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}}.
- {{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.
- {{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}}.
- {{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}}.
- {{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.

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.

Identity Federation

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

- 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}}

Policy

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}}.
- 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}}.

Certificate Management Services

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

The Certificate Management service levels indicate any actions involving the root certificate.

- {{Actor.Name}} created a root certificate.
- {{Actor.Name}} uploaded a root certificate.
- {{Actor.Name}} revoked a root certificate.
- {{Actor.Name}} retrieved a root certificate
- {{Actor.Name}} created a root certificate.

Identity Services

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

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

RAS Services

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

The following RAS 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

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

- {{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}}

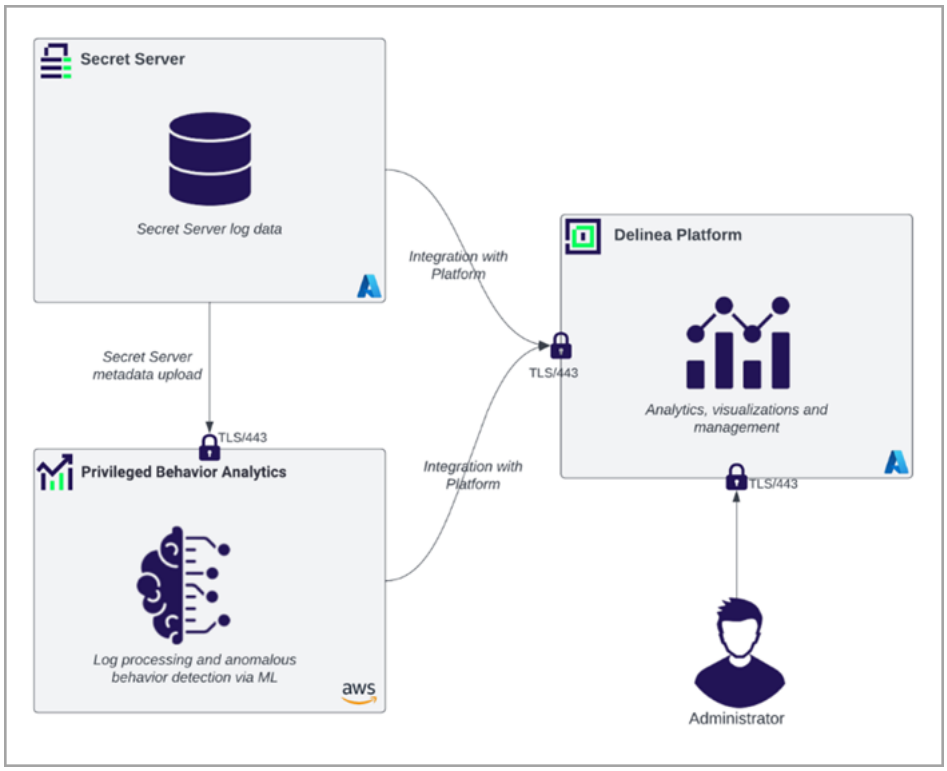
Behavioral Analytics

Important: This feature is currently available only to customers participating in our 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.

Risk Based Behavioral Analytics

Behavioral Analytics (BA) on the Delinea Platform fortifies your enterprise security posture. It applies machine learning algorithms to Secret Server event logs to render visually intuitive graphical displays and risk scores of events and activities. These displays are designed to help administrators and other staff members learn to recognize trends and better respond to security threats.

High Level Architecture



Next, the Requirements section covers the pre-requisites and dependencies for Behavioral Analytics.

Behavioral Analytics Requirements

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

Behavioral Analytics requires administrator privileges on all the following instances:

- Delinea Platform tenant instance
- Secret Server Cloud tenant instance

- Privileged Behavioral Analytics instance

> **Note:** In upcoming releases, a separate instance of Privileged Behavioral Analytics (PBA) will no longer be required, which will simplify onboarding and integration.

Next, the Setup section covers the steps to set up and configure Behavioral Analytics.

Behavioral Analytics Setup

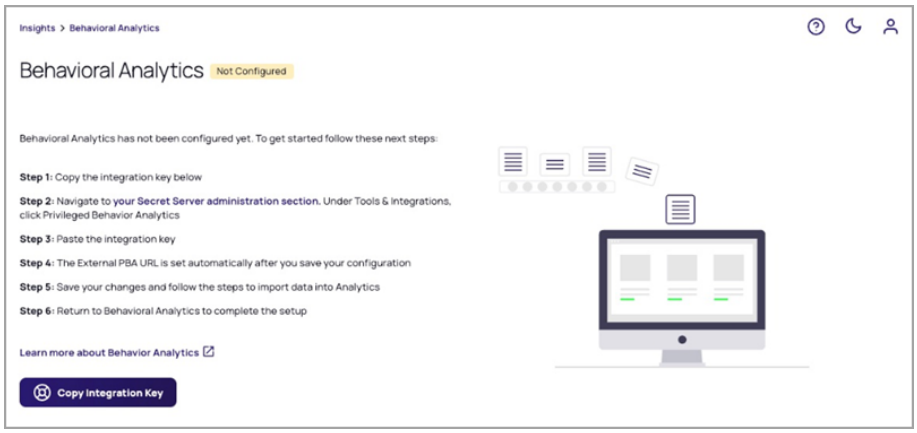
> **Important:** This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

Integrate Behavioral Analytics into Secret Server

To use Behavioral Analytics on the Delinea Platform, you must integrate it into Secret Server using an integration key. The integration key contains the secret access code and other parameters for uploading data from Secret Server to Behavioral Analytics. The integration key is encrypted during transit and when it is saved and entered into Secret Server. This encryption uses standard Secret Server encryption (AES-256, plus DPAPI/HSM if that has been configured).

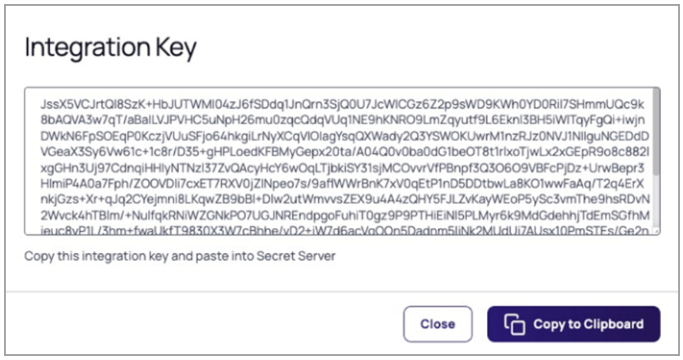
Generate and Copy the Integration Key

1. Log in to the Delinea Platform.
2. Click **Insights** from the left navigation menu, then select **Behavioral Analytics**. The Behavioral Analytics splash screen appears, describing the next steps in the configuration process.



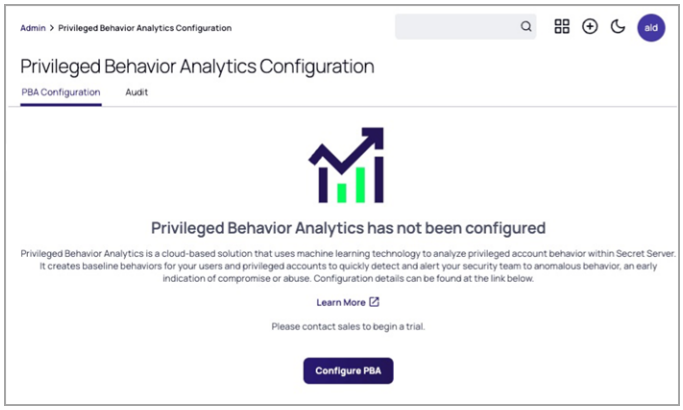
3. Click **Copy Integration Key**.

4. In the Integration Key dialog box, click **Copy to Clipboard**.

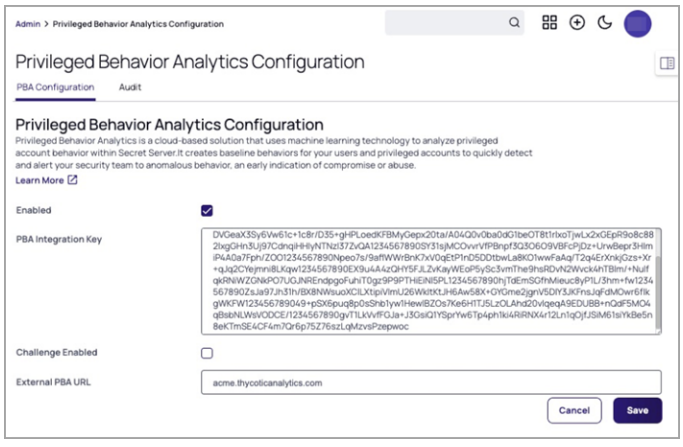


Configure the Integration into Secret Server

1. Click **Settings** from the left navigation, then select **Administration** below Secret Server.
2. Under **Tools & Integrations**, click **Privileged Behavioral Analytics**.
3. On the **Privileged Behavioral Analytics Configuration** page, click the **PBA Configuration** tab.



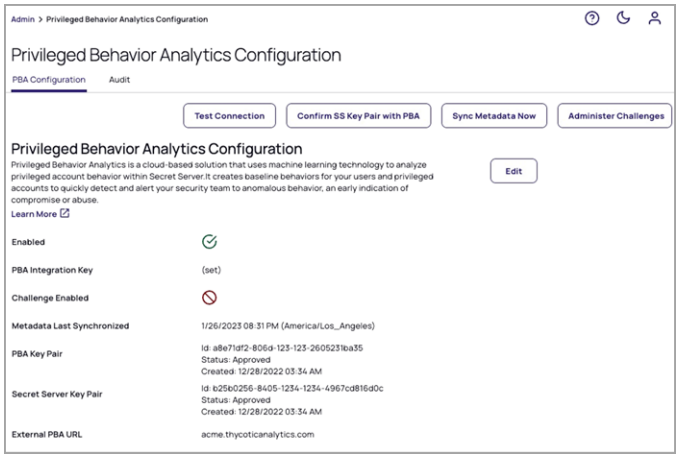
4. Click **Configure PBA**.



5. The page opens to enable configuration.
6. Select the **Enabled** checkbox to enable the Secret Server and Behavioral Analytics integration.
7. In the **PBA Integration Key** box, paste the Integration Key from your clipboard.
8. In the **External PBA URL** box, enter the URL of your Behavioral Analytics cloud instance (for example, `acme.thycoticanalytics.com`). After you save your configuration, this URL will be saved and entered into fields automatically.

   Note: You can leave the **Challenge Enabled** box unselected for now. Support for Secret Server Access Challenges on the Delinea Platform is coming soon.

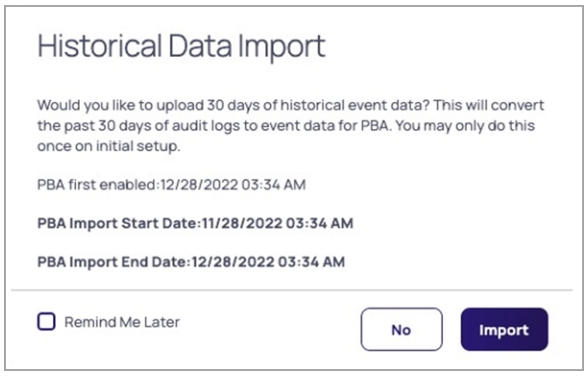
9. Click **Save**. The next dialog displays the details of your PBA configuration.



10. To confirm the configuration, click **Confirm SS Key Pair with PBA**.
11. To test the connection, click **Test Connection**.

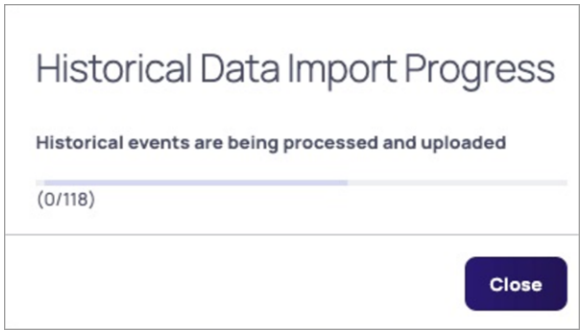
Import Historical Data from Secret Server

When you first enable Privileged Behavioral Analytics, the **Historical Data Import** dialog box appears and asks if you would like to import the last 30 days of historical event data from Secret Server. This is a one-time opportunity to import historical data from Secret Server, which can be used from day one to begin analyzing user behavior.



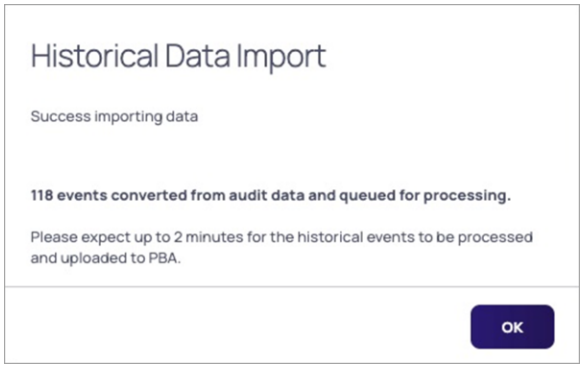
- If you click **Import**, Privileged Behavioral Analytics imports data for the 30-day period immediately prior to the date when you first saved a configuration with Privileged Behavioral Analytics enabled.
- If you select the **Remind Me Later** checkbox, you will see the same prompt the next time you save a configuration with Privileged Behavioral Analytics enabled. To ensure data continuity, the imported data will still be from the same 30-day period immediately prior to the first date you saved a configuration with Privileged Behavioral Analytics enabled.
- If you click **No**, the query is permanently dismissed.

To begin importing the historical data from Secret Server, click **Import**. The **Historical Data Import Progress** dialog appears, displaying the total number of events to be imported, next to the number of events that have been imported so far, which is updated in real time.



When the data import finishes, the **Historical Data Import** dialog appears, indicating the success of the data import process. The dialog also provides an estimate of the time required to convert the audit data to event data and upload it to Behavioral Analytics.

Note: Because audit data is persisted in Secret Server but event data is not, Privileged Behavioral Analytics converts Secret Server's audit log data into event data to facilitate the analysis of user behavior.



Next, Customize Your Behavioral Analytics Settings covers post-configuration steps to customize and tune Behavioral Analytics.

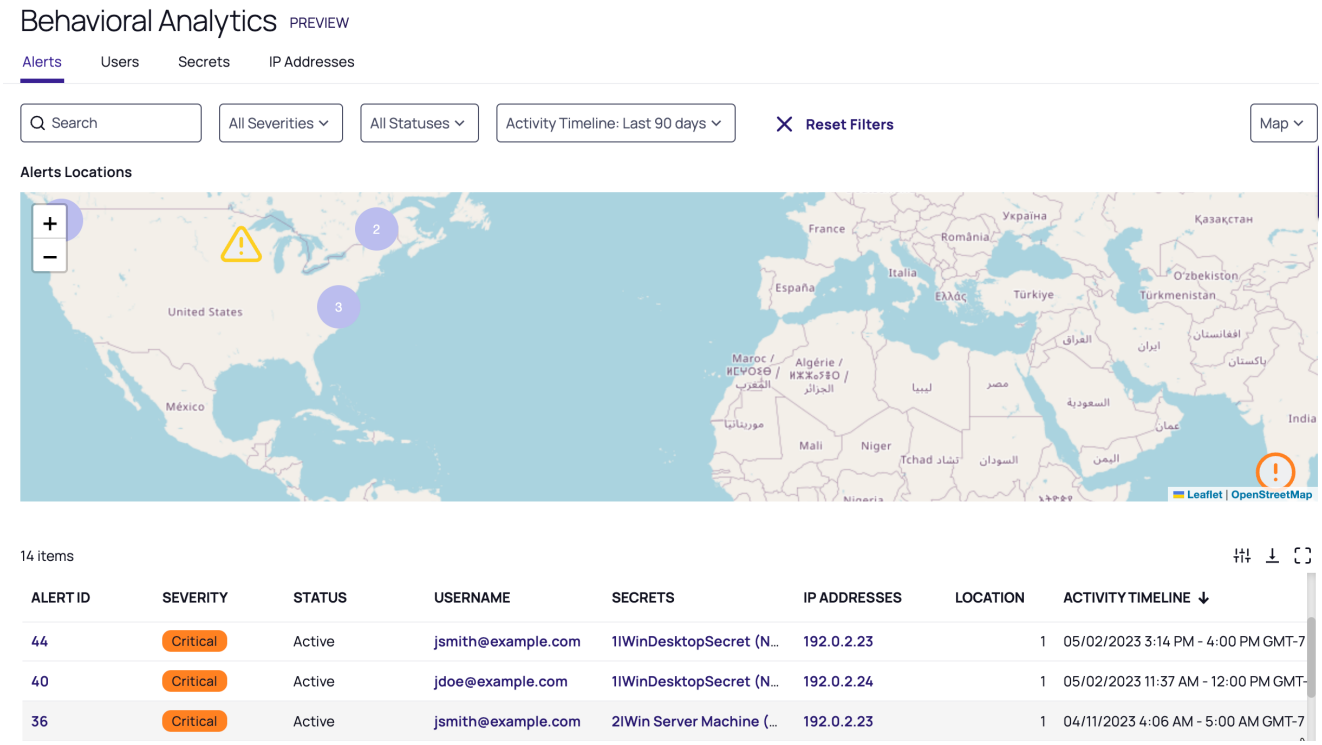
Using Behavioral Analytics

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

To navigate the main Behavioral Analytics page, click **Insights** from the left navigation menu, then click **Behavioral Analytics**. This page serves as a dashboard for overseeing the analytics functions. It provides breadcrumb navigation, search capabilities with filters, interactive risk maps and charts, and drill-down capabilities into behavior details.

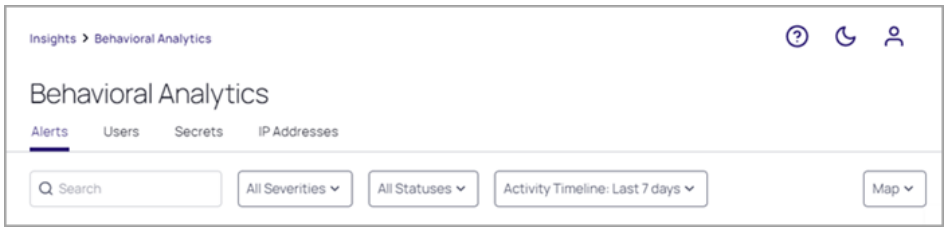
Alerts Page

The main Behavioral Analytics page opens by default to the **Alerts** tab, where you can view the analytics by alerts. To view the analytics by **Users**, **Secrets**, or **IP Addresses**, click the respective tabs.



Search for Alerts

To search for alerts, enter text into the Search box. To filter your search results by severity, status, or activity timeline, select filter options from the drop-down boxes to the right of the Search box.



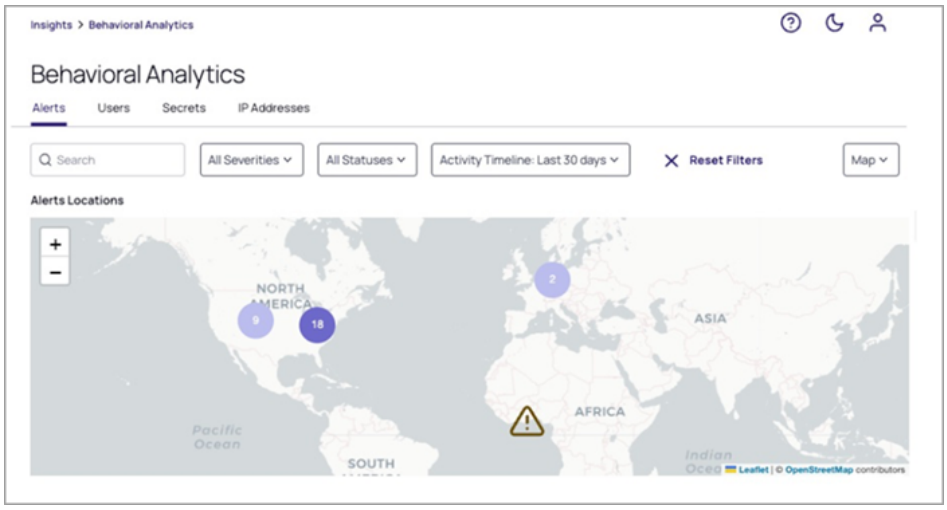
Choose Your Display

To select the way alerts are graphically displayed, select **Map**, **Bar**, **Line**, or **Heat Map** from the drop-down box to the right of the search options.

To review additional details about each alert, click to interact with the data presented on the map, bar chart, line chart, or heat map.

Map View

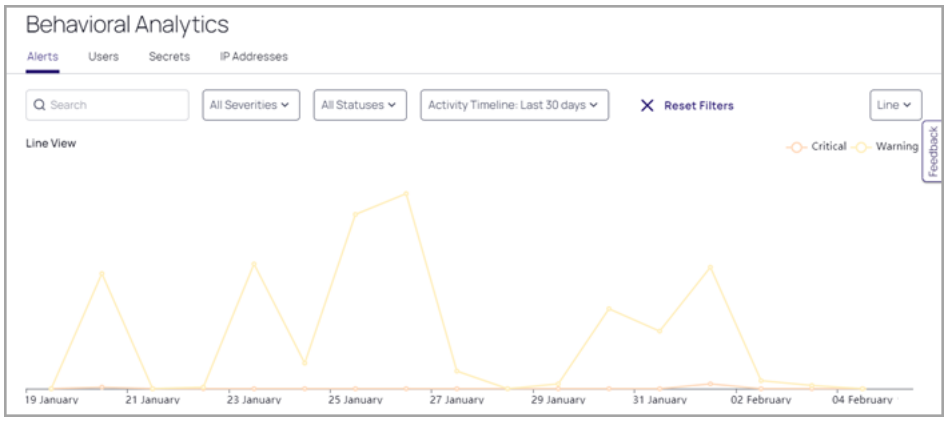
The Map view reveals the locations where alerts originated. If two or more alerts exist close to each other geographically, a purple circle appears on the map to represent the cluster, with the number of alerts in the cluster displayed in the center.



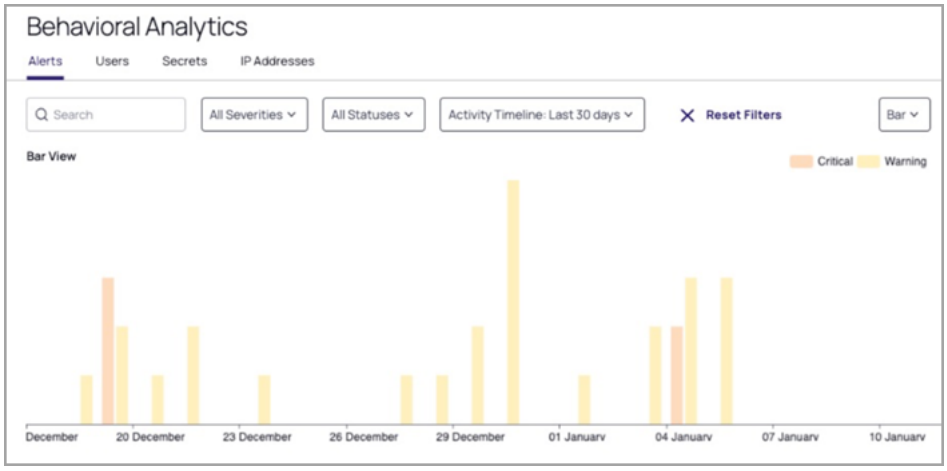
Map View Legend

- Warning Alerts ⚠
- Critical Alerts ⓘ
- Alert Clusters 11

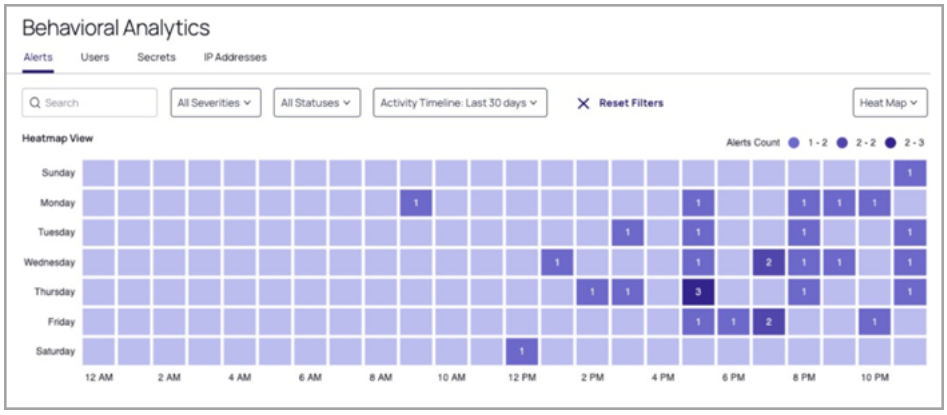
Line Chart View



Bar Chart View



Heatmap View



Alerts Table

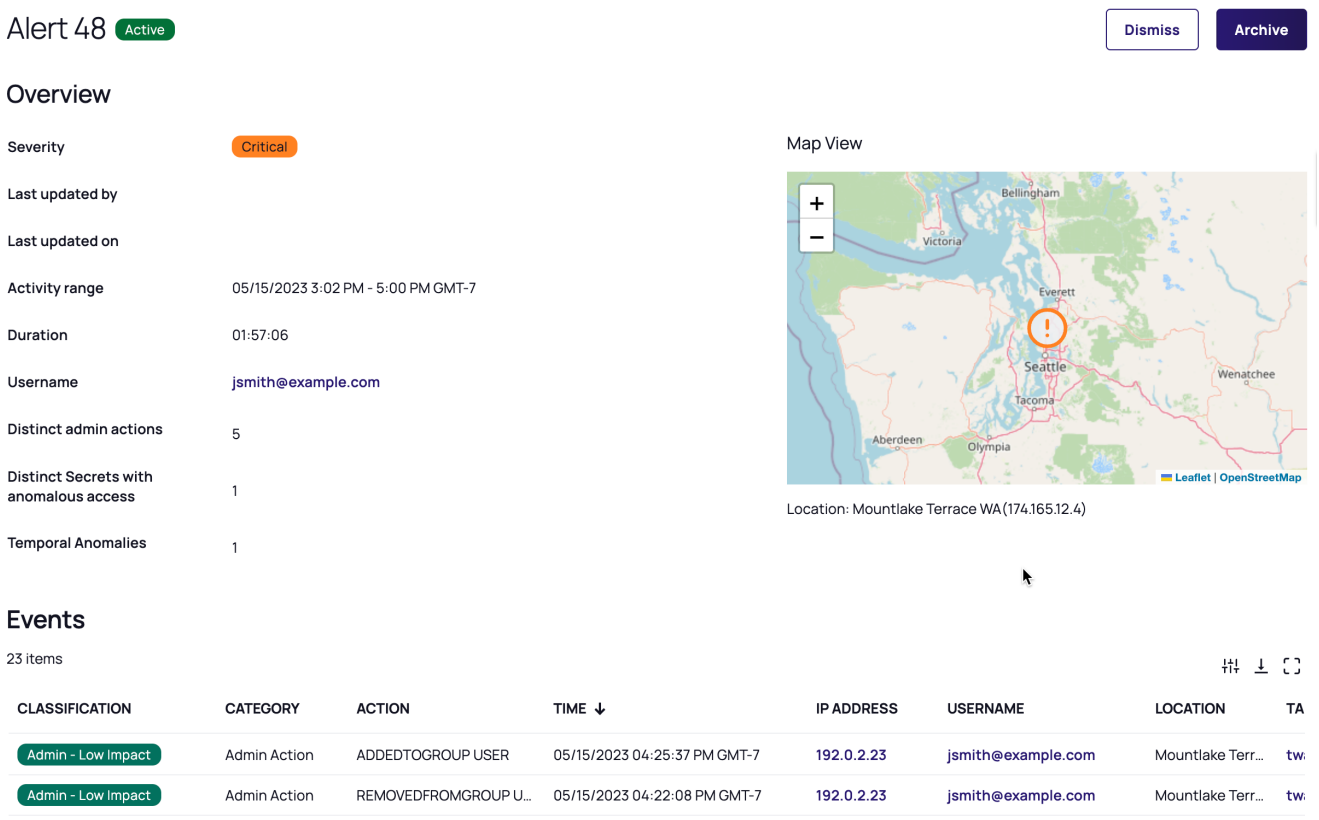
At the bottom of the Alerts page is a table listing each alert in a row, configured with thresholds to trigger a Warning or Critical alert (see Alert Settings). The information presented in the table columns is described below. Four data items in each row are in bold purple text, indicating that you can click them to see additional details. They are **Alert ID**, **User Name**, **Secrets**, and **IP Address**. Those details are covered in sections below.

The table below describes the content in each column.

Column	Description
Alert ID	Unique alert ID
Severity	Whether the event is flagged as Critical or Warning
Status	Alert status: Active, Dismissed or Archived
User Name	The Secret Server user who caused the alert; clicking their name opens the User Details page
Secrets	List of secrets from the events that are part of the alert
IP Addresses	The IP addresses used during the alert period with links to each IP Details page
Location	Count of distinct IP addresses from those events
Activity Timeline	The time span within which the Alert occurred

Alert Details View

To review more details of a specific alert, click the alert in the **Alert ID** column. The Alert details view appears. The details are further explored in the sections below.



Alerts Actions

At the top of the Alert details page, the Alert ID and its action are displayed.

The actions are described in the table below.

Action Name	Description
Activate	Reactivating this alert will change its status on the main alerts table. You can re-archive or dismiss this alert later.
Dismiss	Dismissing this alert will normalize this pattern of secret access for the user. If the user takes similar action in the future, you will not be alerted. This action cannot be undone.
Archive	Archiving this alert will deactivate the alert. Archived alerts can still be reviewed from the main alerts table. The system will continue to see this type of behavior as anomalous for this user and alert.

Overview Section

Below the Alerts Actions is an **Overview** section providing details described in the table below:

Overview Field	Description
Severity	Critical, Warning for the alert
Last Updated By	Who last updated the status of the alert
Last Updated On	Date the alert was last updated
Activity Range	Earliest to latest dates of the alert events
Duration	The time span on the activity range
Username	Username for the account on the activity
Distinct Admin Actions	Count of distinct admin actions in the events actions
Distinct Secrets with Anomalous Access	Count of distinct secrets that had anomalous activity anomalous access

Overview Field	Description
Temporal Anomalies	A time entry will be listed here if the Alert occurred at a time the User does not normally access the Secrets involved in the Alert; clicking on the time entry will display the User's Temporal Data.

Events Section

In the middle of the Alert details page is the **Events** section, providing details described in the table below:

Event Column	Description
Classification	For secret access, the following classifications are possible: "Anomalous" or "Normal". For administrative actions done on a secret, the following classifications are possible: "Admin - ", Low, Normal, High or Critical Impact
Category	Categorization of the event: a secret access, or the action in case of an administrative action
Action	The action taken in case of a secret access, or in the case of an administrative event, the administrative action taken
Time	The date and time of the event
User Name	User name for the user performing the action
Location	The geo location looked up for the IP address above
Target	The name of the secret from Secret Server
Info	Additional information about the action, for example, what field from the secret was examined.

Notes Section

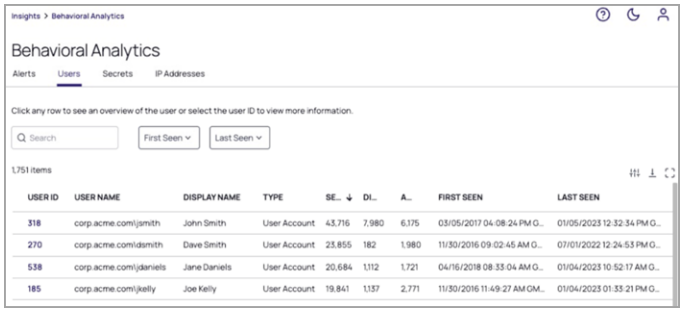
At the bottom of the Alerts details page is the **Notes** section, where users can create notes pertaining to the alert.

Notes Column	Description
Author	User who added a note to the alert
Created	When they wrote the note
Note	Content of the note

Users Page

1. Click **Insights** from the left navigation, then select **Behavioral Analytics**.
2. Click the **Users** tab.

The **Users** page lists all User IDs, their Display Names, Account Type, total number of times they have accessed or modified Secrets, number of unique Secrets they have accessed, total number of administrative actions they have performed, when they were first seen in Behavioral Analytics, and when they were last active.



User Details View

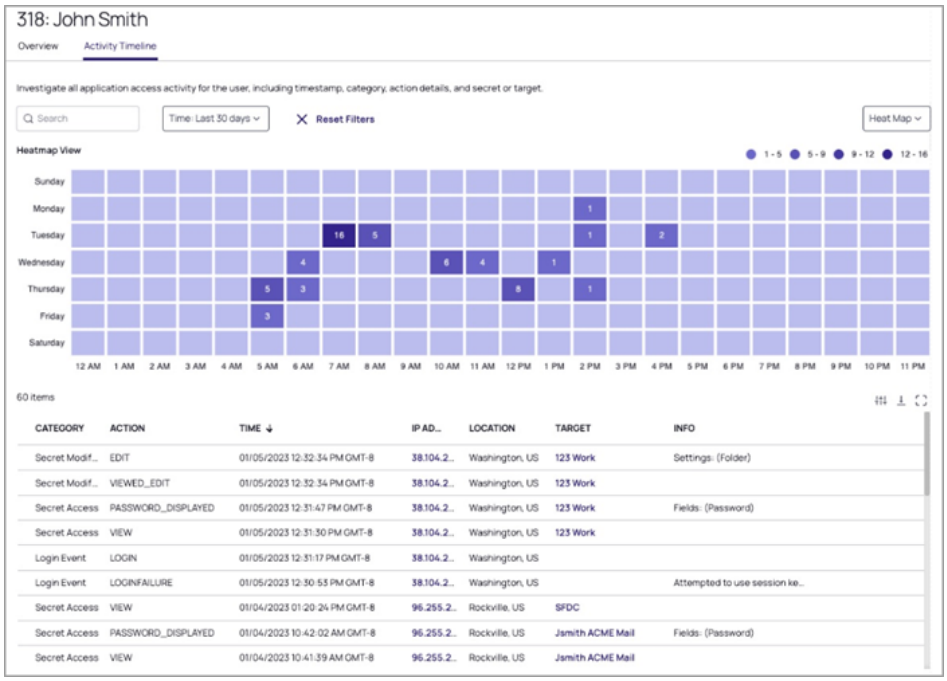
Click an entry under the **User ID** column to open the user details view, where you can dive deeper into a specific user's behavior from the perspective of many types of data collected on them.

Overview

The user details view opens by default to the **Overview** tab, which displays information about the user including their Display Name, Email, User Name, User ID, total secret events, activity range, last secret event, and groups.

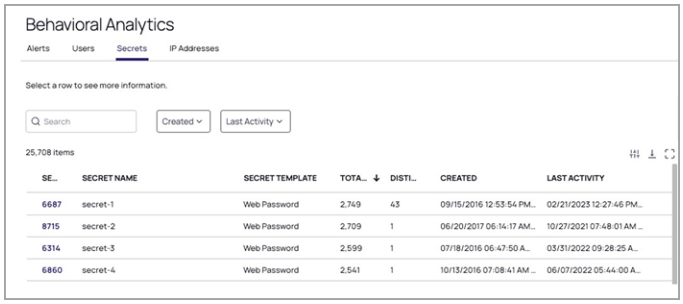
Activity Timeline

Click the **Activity Timeline** tab to view interactive graphical and tabular displays of information on the user's actions, including when they took them, where they were when they took them, and what secret they used.



Secrets

The **Secrets** tab lists all secrets used, with each secret in a row and basic information displayed under columns.

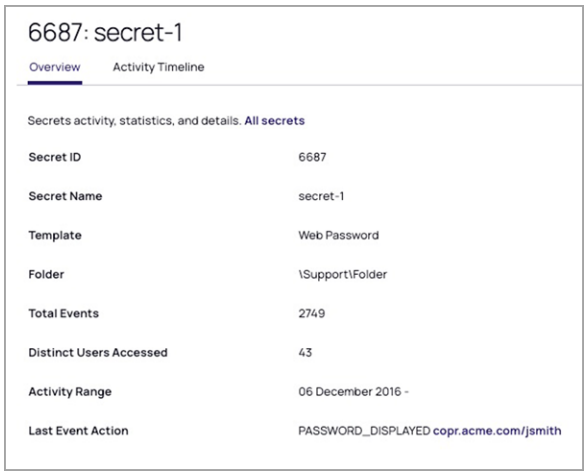


Secret Details View

To view additional details about a secret and how it is being accessed, click a secret in the **Secret ID** column. The secret details page can be used to investigate how a secret is being accessed from the perspective of many types of data collected on it.

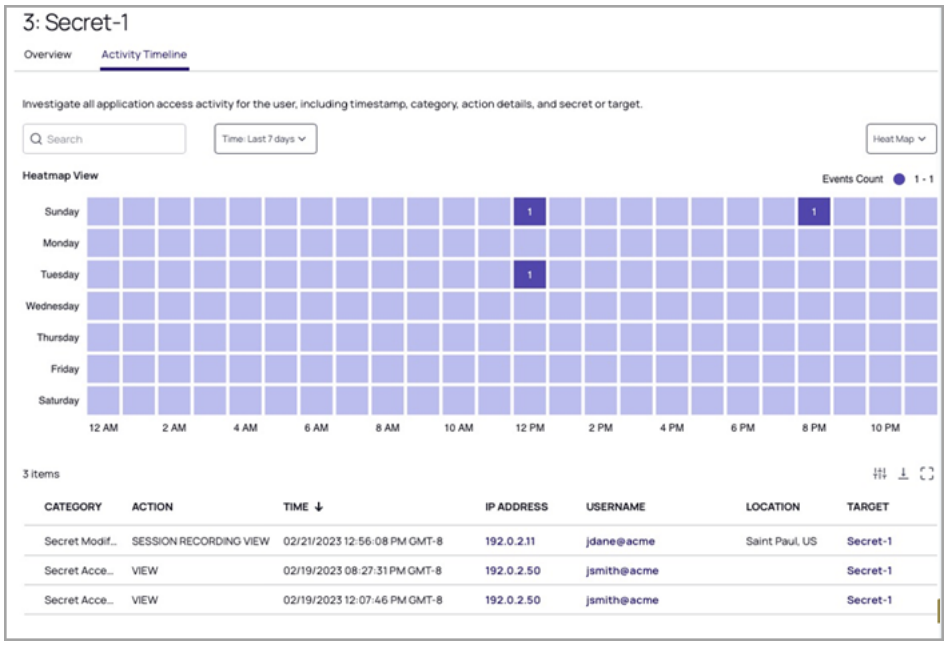
Secret Overview

The secret details view opens by default to the **Overview** tab, which lists key information including Secret ID, Secret Name, Secret Template, Folder, the total number of events (Secret accesses plus modifications), number of Distinct Users that have accessed the Secret, the Activity Range, and the Last Event Action.



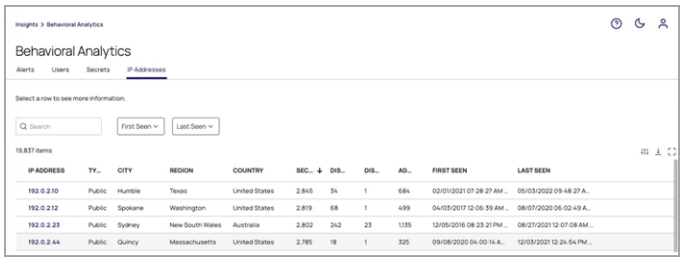
Activity Timeline

The Activity Timeline tab provides interactive graphical and tabular displays of information on a specific secret, including when it was used, where it was used, who used it, and what secret was used with it. It also displays alerts, warnings, accesses, and modifications, as well as timestamps, IP address, and event details.



IP Addresses

The IP Addresses tab lists all IP address used on the platform, with each IP address in a row and basic information listed in columns, including its type (Public or Private), Status, City, Region, Country, the number of secret accesses plus modifications, the number of unique secrets accessed, the number of unique users accessing secrets, the number of administrator actions performed (including logins), and the first and last time Behavioral Analytics observed the IP address in data.

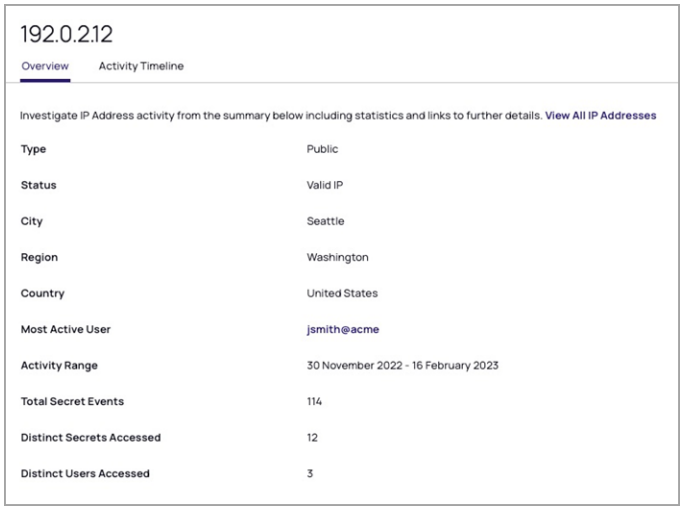


IP Address Details View

To see more details about a specific IP address, click a numeric address under the **IP Address** column.

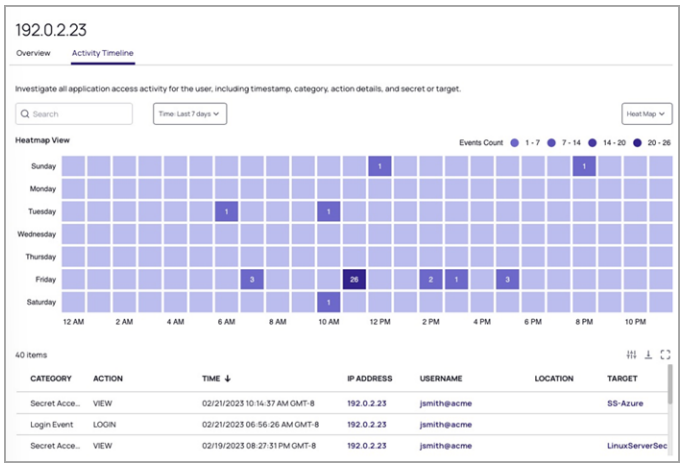
Overview

The IP Address details view opens by default to the **Overview** tab which dislayes additional information about the IP address, including the **Most Active User** and **Activity Range**.



Activity Timeline

The Activity Timeline tab provides interactive graphical and tabular displays of information on a specific IP Address, including when it was used, who used it, and what secret they used with it.



Behavioral Analytics Customization

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

Most analytics customizations and administrative tasks can be accomplished from the Behavioral Analytics page (**Settings** > **Behavioral Analytics**), including adjusting the alert thresholds and reconfiguring the integration with Secret Server as needed.

Alert Settings

Events generate **Warning** or **Critical** alerts according to the severity thresholds you set. Events that fall outside these thresholds are considered **Normal**.

Thresholds are represented as sensitivity levels ranging from least to most sensitive. For instance, setting the **Warning** alert threshold to **Least Sensitive** will set a numerical value stored in the platform tenant. Those values are used to determine what alert, if any, should be issued.

If the risk score exceeds the Warning threshold value, a warning alert is issued. If it exceeds the Critical threshold value, a Critical alert is issued.

For Behavioral Analytics on the Delinea Platform, the threshold values for sensitivity levels were devised so that a customer could edit those thresholds, either in the PBA console or in the Delinea Platform portal, and they would be consistent.

In the PBA console, customers are allowed to set either threshold to a value between 2 and 50. With the constraint that the Alert (Critical) threshold must be larger than the Warning threshold. That behavior is preserved in the Behavioral Analytics for Platform API and portal.

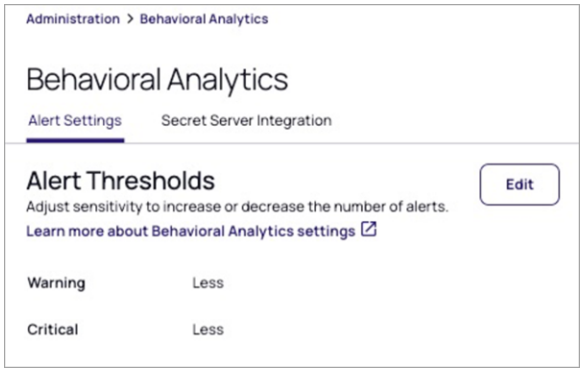
The API code uses settings from the table below to set the threshold values and to read what may be a numeric value entered from the Standalone console, then to map it to the least-to-most sensitive levels.

Sensitivity	Warning	Critical
Most Sensitive	2	7

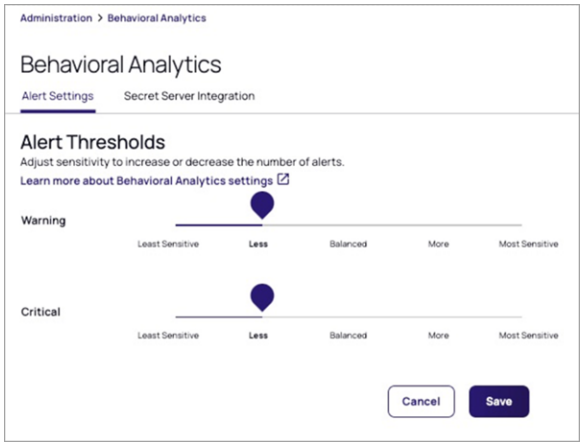
Sensitivity	Warning	Critical
More	6	13
Balanced	10	20
Less	14	28
Least Sensitive	18	38

To adjust the thresholds for generating Warning or Critical alerts, follow the steps below.

1. Click **Settings** on the left navigation menu, then select **Behavioral Analytics**.
2. Click the **Alert Settings** tab.



3. Click **Edit**.
4. Click and drag the indicator to the desired sensitivity. Be default, both Warning and Critical alert thresholds are set to **Balanced**.



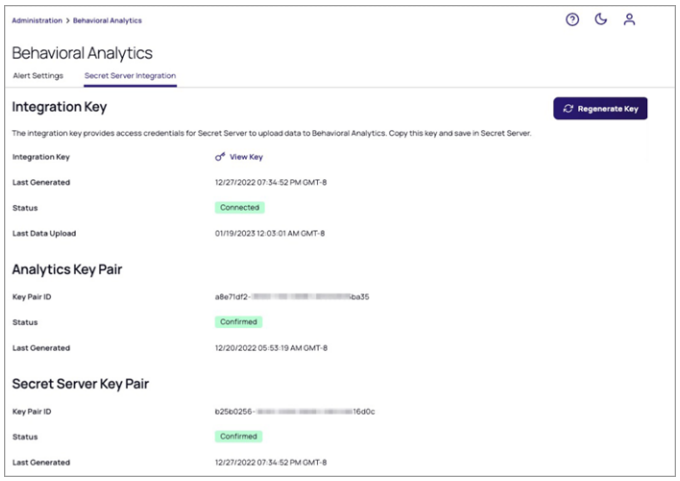
Severity	Description
Warning	An alert raised based on the risk score, compared to the threshold. A Warning alert will be raised if Risk Score >= Warning < Critical.
Critical	An alert raised based on the risk score, compared to the threshold. A critical alert will be raised if Risk Score >= Critical.

Note: No alert will be raised if Risk Score < Warning.

Secret Server Integration Settings

To configure secure communications between Secret Server and Behavioral Analytics, follow the steps below.

1. Click **Settings** from the left navigation menu, then select **Behavioral Analytics**.
2. Click the **Secret Server Integration** tab.



Integration Key Section

- **Regenerate Key** button: To regenerate the Integration Key, click **Regenerate Key**. 

  A key rotation process is initiated in which both Secret Server and Privileged Behavioral Analytics generate a new key pair, and use the previous public key to exchange the new pair with each other. After you regenerate the integration key, you will need to copy it to your Secret Server instance again, to start the initial key exchange.
- **Integration Key** field: To view and copy the Integration Key, click **View Key**. The Integration Key is copied to Secret Server to provide the credentials and configuration information required to enable the uploading of log data from Secret Server to Behavioral Analytics. See the *Generate and Copy the Integration Key* section, above.
- **Last Generated** field: Displays a timestamp indicating the last time the key was generated.
- **Status** field: Displays one of two states described below.

Status	Description
Not configured	Not Connected. Behavioral Analytics has not been configured yet.
Connected	Behavioral Analytics has been configured and connection has been established.

- **Last Data Upload** field: Displays a timestamp indicating the last time data was transferred from Secret Server to Behavioral Analytics.

Analytics & Secret Server Key Pair Sections

The **Analytics Key Pair** and **Secret Server Key Pair** sections use the same fields in the same ways, so they are described together below.

- **Key Pair ID** fields: Used by Privileged Behavioral Analytics during Single Sign On to verify Secret Server's user claims as an identity provider. In the opposite direction, it is used by Secret Server as an added layer of security to verify that Access Challenges were signed by the authorized Privileged Behavioral Analytics instance.
- **Status** fields: Displays one of three states:

Status	Description
Not available	Key pair has not yet been generated.
Pending	Key pair has been generated, but is awaiting confirmation by Secret Server.
Confirmed	Key pair has been confirmed by Secret Server.

- **Last Generated** fields: Displays a timestamp indicating the last time the key pair was generated.

Roles Settings

Behavioral Analytics offers a set of permissions that can be leveraged via the existing, built-in roles of *Platform Administrator* or *Platform Auditor*. Custom roles can be created to leverage specific permissions based on your requirements. The table below describes the built-in roles and associated permissions for each.

Roles can be managed by clicking **Access** from the left navigation menu, then selecting **Roles**.

For more information, see User Roles and Permissions

Platform Administrator

Role Permission	Description
delinea.platform/analytics/settings/manage	Can view and manage Behavioral Analytics settings

Role Permission	Description
delinea.platform/analytics/settings/create	Can create all Behavioral Analytics settings
delinea.platform/analytics/settings/delete	Can delete all Behavioral Analytics settings
delinea.platform/analytics/settings/read	Can view all Behavioral Analytics settings
delinea.platform/analytics/settings/update	Can update all Behavioral Analytics settings

Platform Auditor

Role Permission	Description
delinea.platform/analytics/read	Can view Behavioral Analytics
delinea.platform/analytics/events/read	Can view event details
delinea.platform/analytics/notes/create	Can create a note
delinea.platform/analytics/notes/delete	Can delete a note
delinea.platform/analytics/notes/read	Can read a note
delinea.platform/analytics/notes/update	Can update a note
elinea.platform/analytics/alerts/update	Can dismiss and archive alerts
delinea.platform/analytics/alerts/read	Can view alert details

Next, Using Behavioral Analytics describes how to use Behavioral Analytics to increase security in your organization.

Marketplace

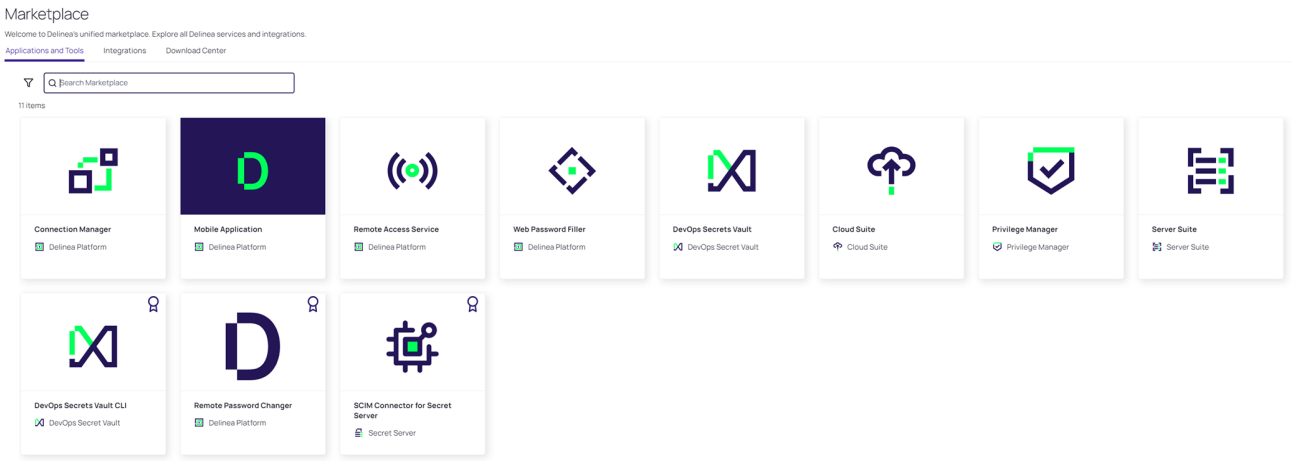
We've designed the Delinea Marketplace as an integration ecosystem for shared services. Marketplace is where you can find applications, scripts, utilities, and other software that you can use with the Delinea Platform. By default, the Admin User role has access to Marketplace and they can control Marketplace access permissions for users.

From the left navigation menu, click **Marketplace**. At the top of the Marketplace home page is a **Search** box where you can enter keywords to search for applications, tools, and integrations. The Marketplace home page has three tabs: **Applications and Tools**, **Integrations**, and **Download Center**.

Applications and Tools

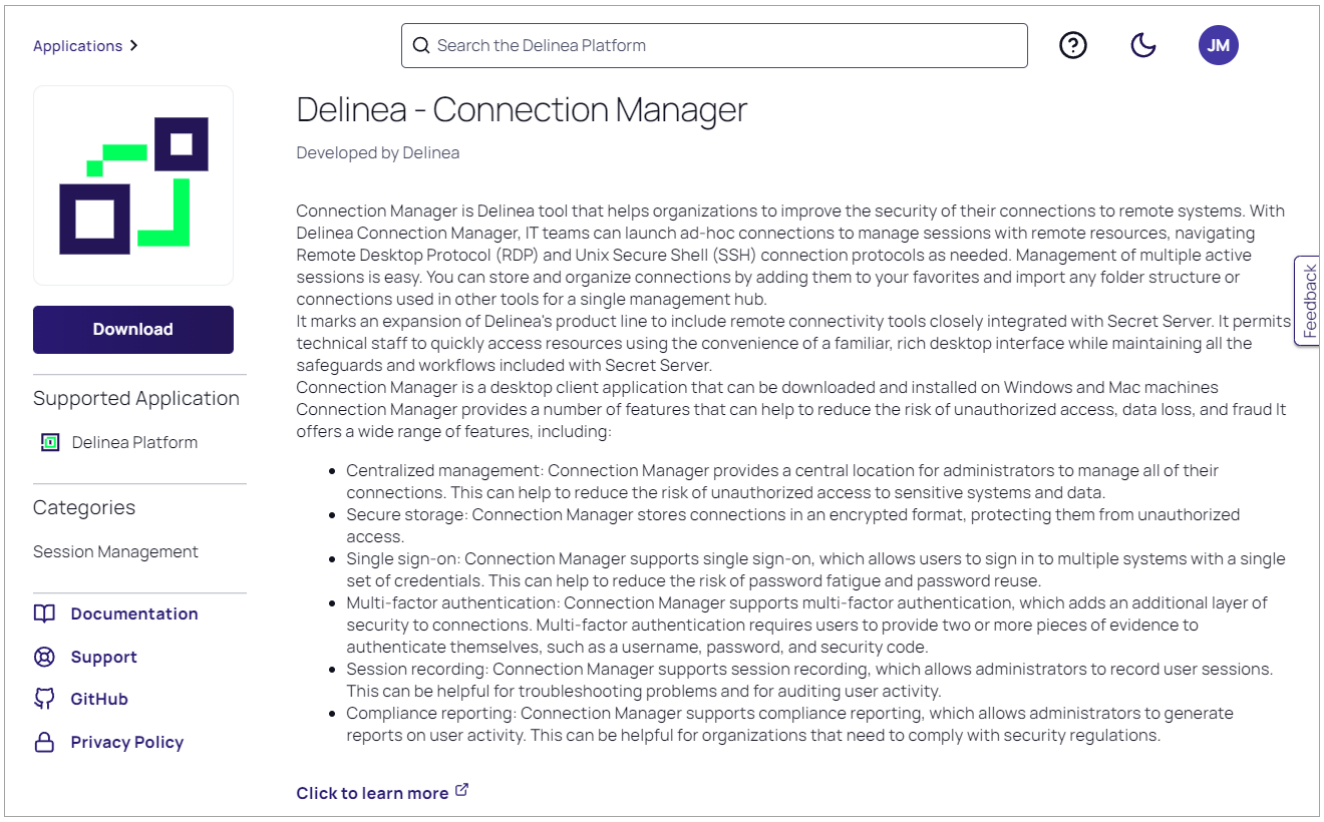
By default, the Marketplace home page opens to the Applications and Tools tab.

Marketplace



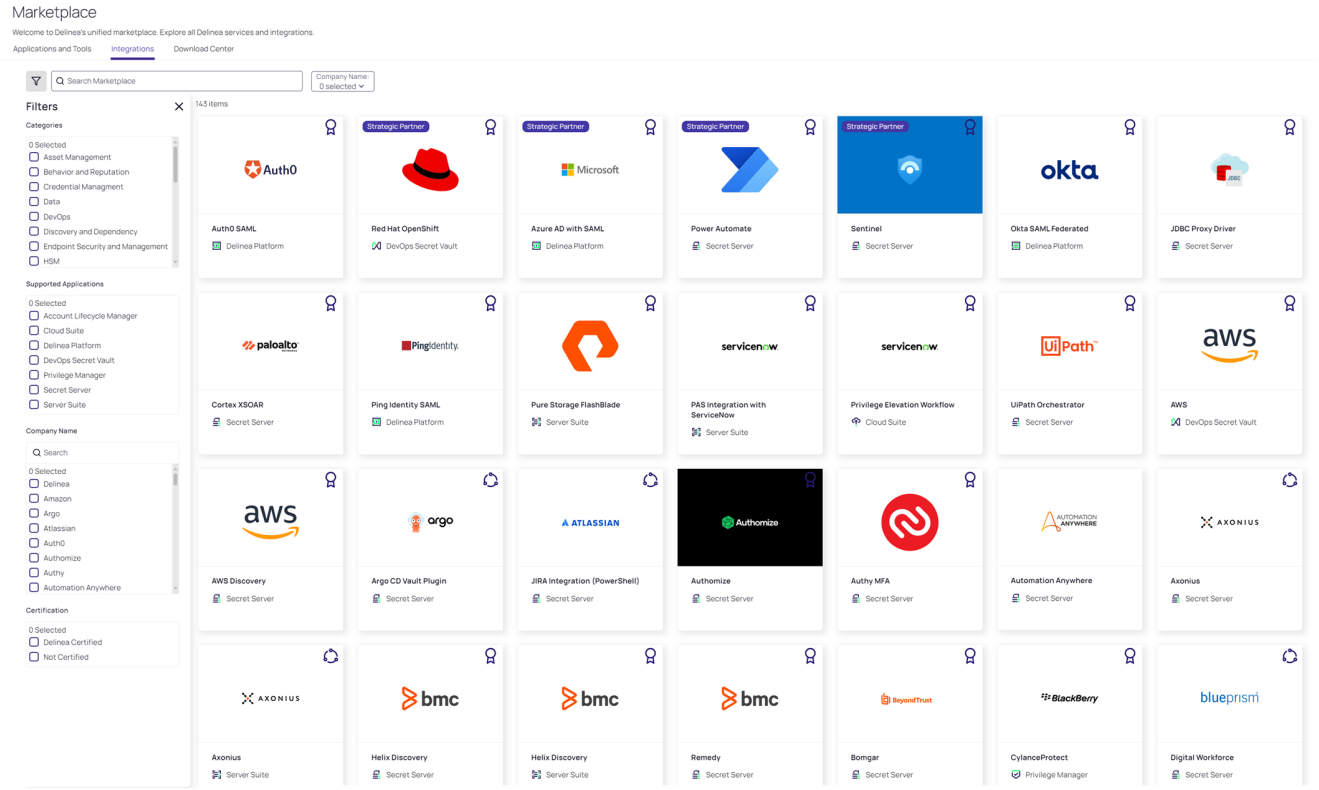
Each available application and tool appears on a card. You can also search for applications by using the Search box below the **Applications and Tools** tab, or by clicking the filter icon to filter your results.

When you click an Application and Tools card, a page opens presenting details about the application, including who developed the application, an application overview, the supported application(s), and application categories. Each application detail page also includes links to the application documentation, support services, Delinea's GitHub site, and the privacy policy.



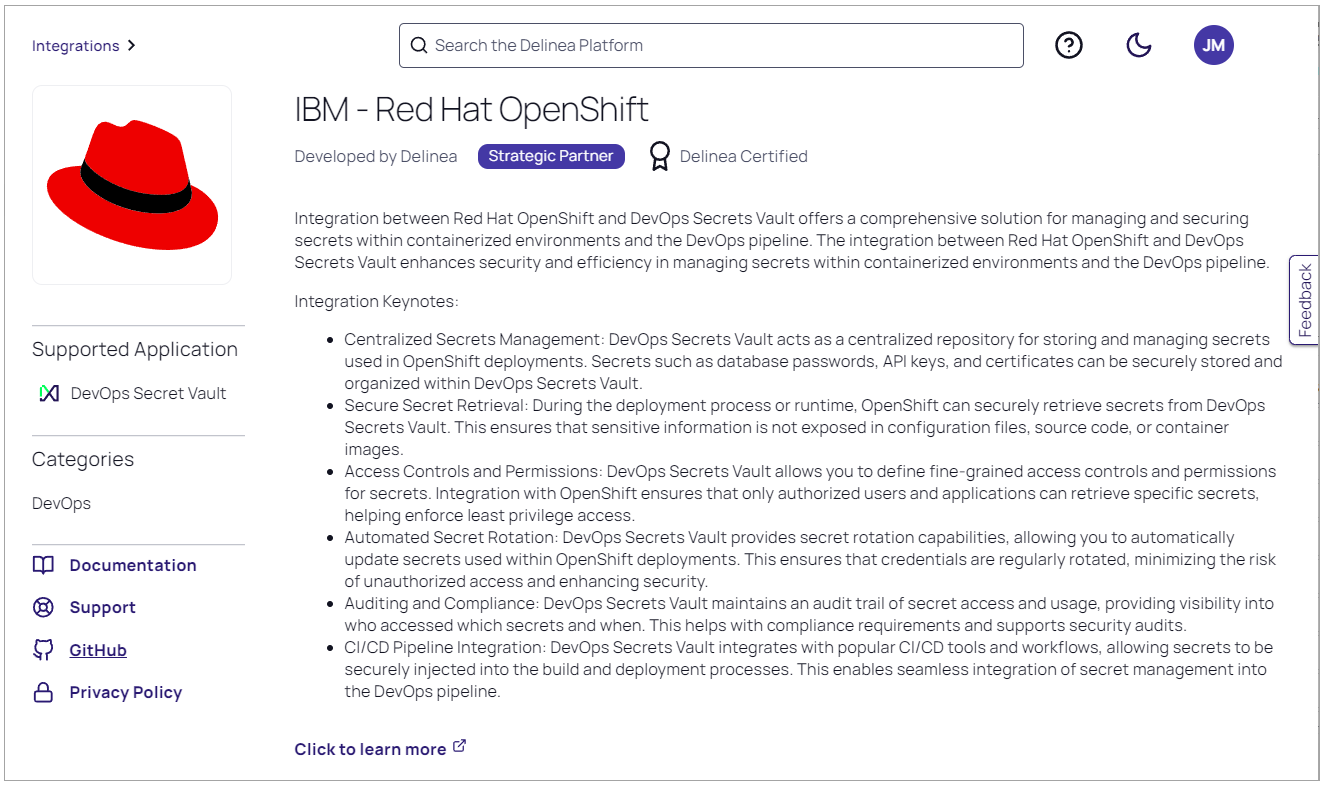
Integrations

From the Marketplace home page, click the **Integrations** tab.



Each available integration appears on a card. You can also search for integrations by using the Search box below the **Integrations** tab, or by clicking the filter icon to filter your results.

When you click an Integrations card, a page opens presenting details about the integration, including who developed the integration, an overview of the integration, the supported application or applications, and the category or categories of the integration. Each integration detail page also includes links to support services, Delinea's GitHub site, the privacy policy, and documentation for the integration and its supported application(s).

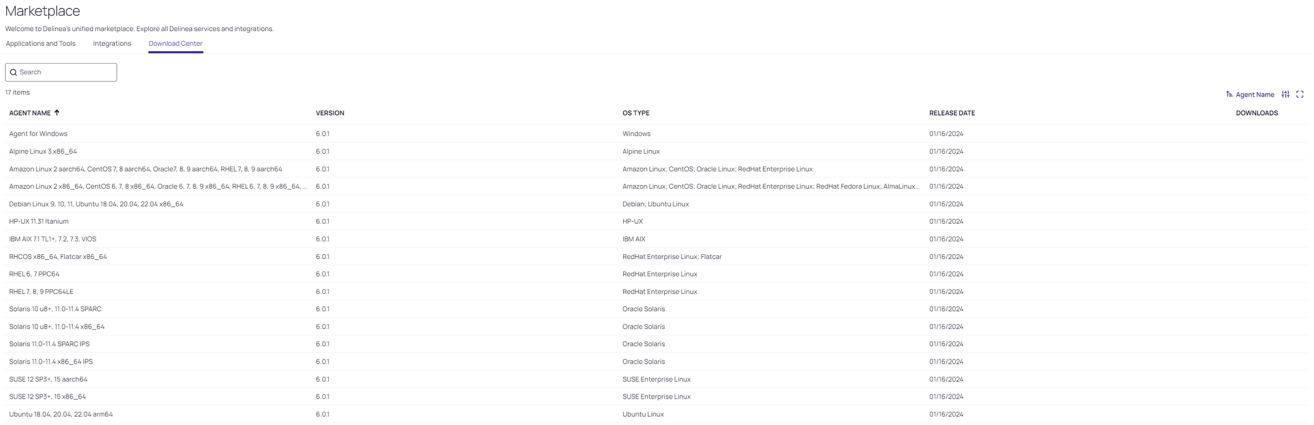


We will always be adding new features, applications, tools, and integrations to the Marketplace, and we expect the available options to grow rapidly.

Download Center

Note: Currently, the Download Center tab is available only to customers using Privilege Control for Servers.

The **Download Center** tab in the Marketplace represents a repository for all downloadable software products, updates, and patches available for Delinea Platform users. With the help of the Download Center, you can obtain the latest version of a product software integrated with Delinea.



To search for the necessary product software, use the Search box displayed on the page. You can also use the filter menu to display product software by Download name, Version, OS type, Release date, or Downloads. Click the download icon for the selected product software to get the software package on your computer.

Webhooks

Important: This feature is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this feature, ask our support or account team for details.

Webhooks enable communication from the Delinea Platform to most third-party Security Information and Event Management (SIEM) applications. Various events and actions in Platform automatically send data to a webhook that a specified SIEM application can gather for analysis and correlation with other security data, providing deeper insights into privileged account activity and helping to identify potential threats faster.

Webhook content is structured in JSON format and is sent to a specified URL.

Current Capabilities

Webhooks are continually being enhanced and expanded. Current capabilities cover **Audit event forwarding**.

Future capabilities will cover an expanded range of events and actions.

Delinea Platform SIEM Integrations

Delinea Platform webhooks integrate with numerous SIEM applications. The configuration articles below cover some of the most common vendors. If your preferred SIEM vendor isn't listed, you can still configure it. Use the official documentation from your vendor and the basic information provided in the previous section as long as your SIEM application accepts data in JSON format.

Webhooks Management

Ensure you have Admin permissions on the Delinea Platform.

Note: Currently, only 10 webhooks can be created per tenant.

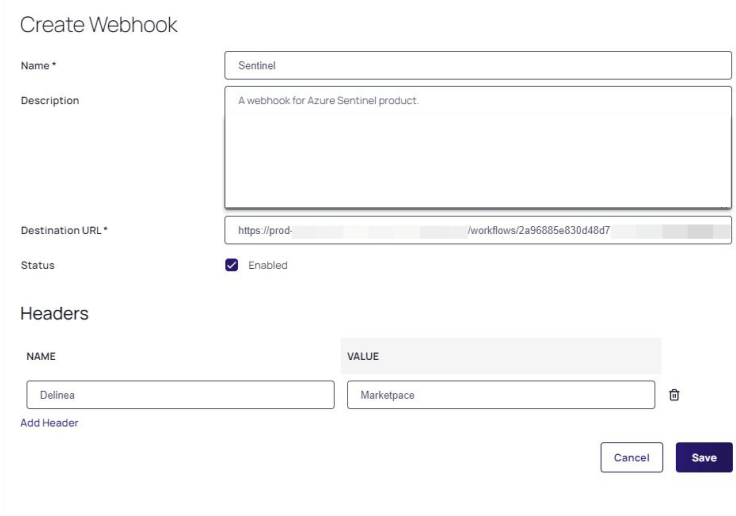
Creating a webhook

Note: Newly created webhooks are enabled by default.

To create a webhook:

1. Log in to the Delinea Platform.
2. Click **Settings** from the left navigation.
3. Click **Webhooks** under **General Setup**.

4. On the Webhooks page, click **Create Webhook**.



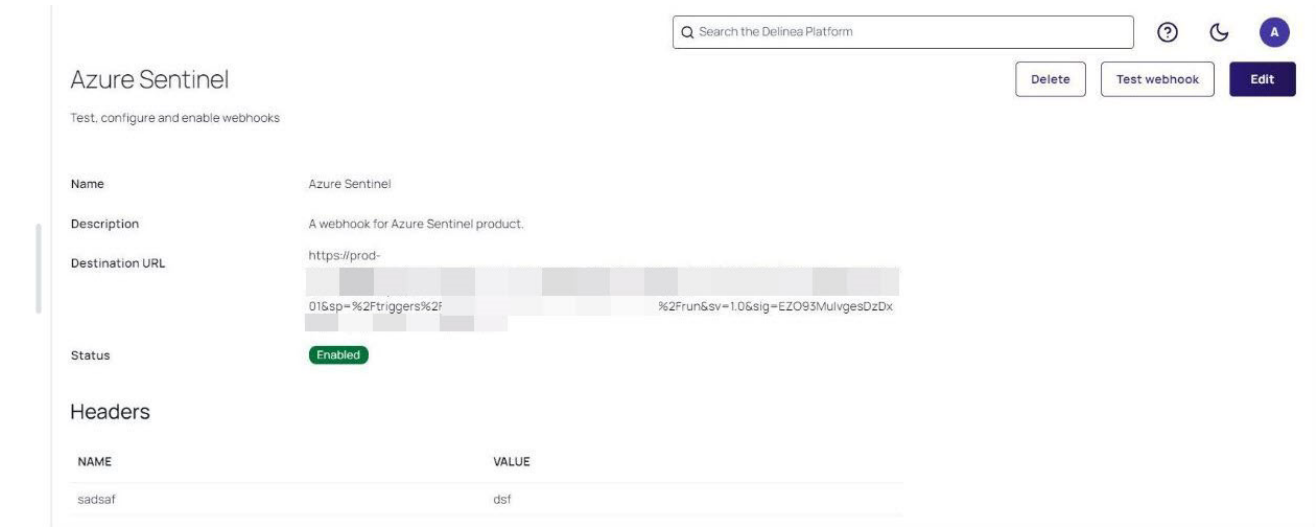
5. Provide the details specified in the table below.

Field	Description
Name	A title for the webhook. The maximum number of characters allowed is 100.
Description	Notes about the webhook. The maximum number of characters allowed is 1,000.
Destination URL	A valid URL to which logs will be sent.
Status	This check box enables or disables the webhook. It is enabled by default. If you disable a webhook and later re-enable it, only subsequent events will be sent.
Header Name	A unique URL token value to use for the URL authentication.
Header Value	A URL token value to use for the URL authentication.

6. **Save** the changes.

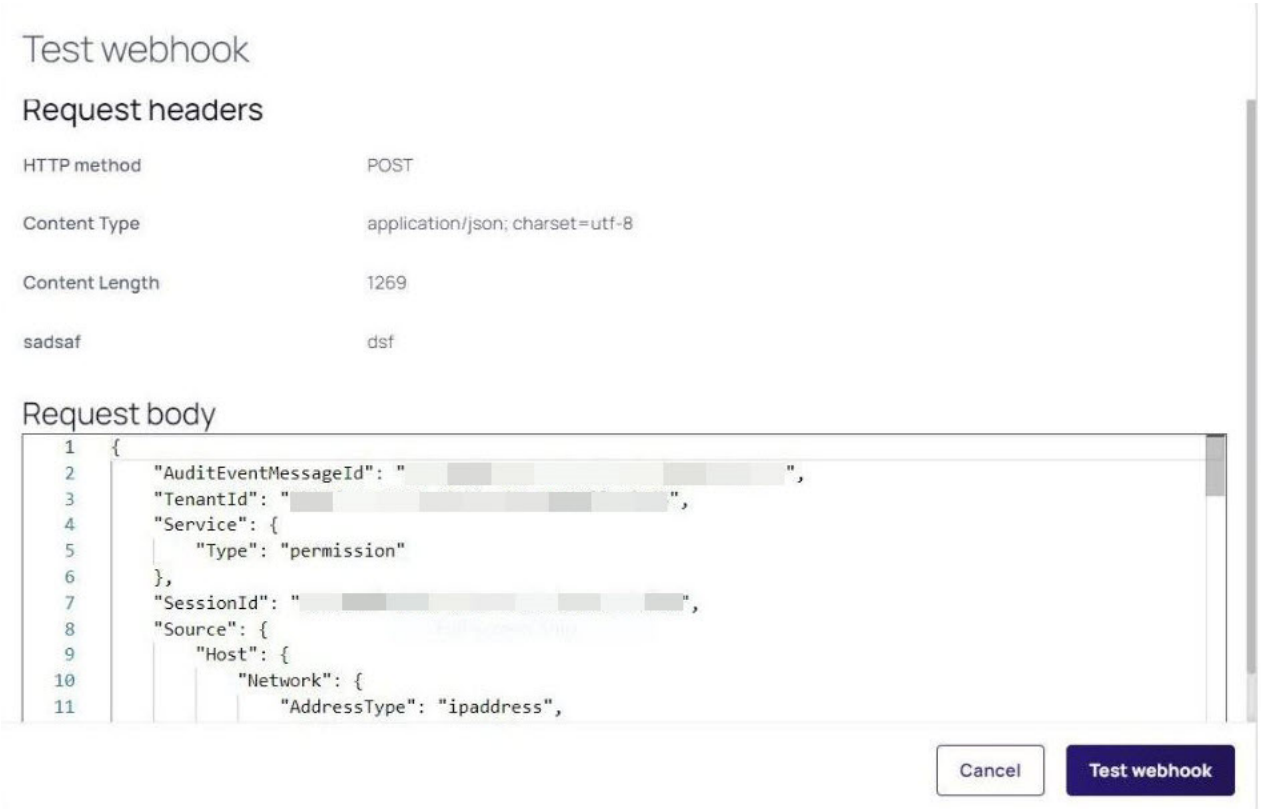
Testing a Webhook

After creating a new webhook, use the **Test webhook** option to verify whether the destination URL is correct, and the connection is successful.



A dialog will display the sample API payload (**Request headers** and **Request body**) to be sent by the webhook.

To initiate the test, click **Test webhook**. The test may take a few minutes. You can return to the main list of webhooks and initiate other tests without interrupting the current one.

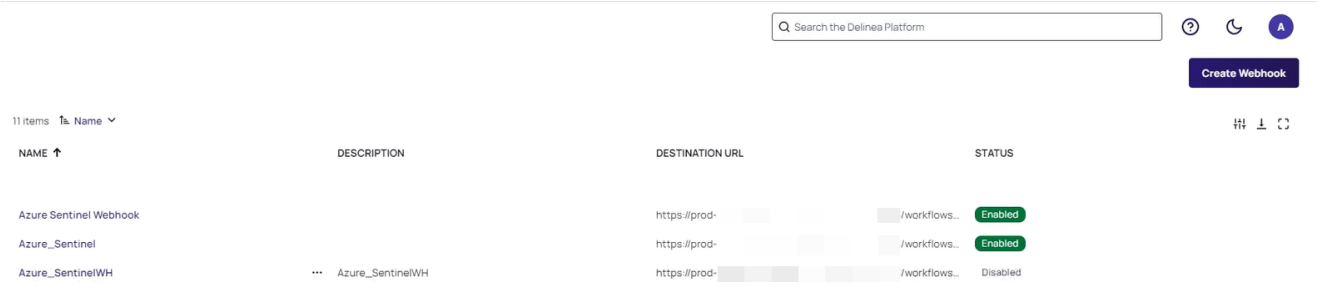


If the test is successful, you will see a corresponding notification. A message with the error details for troubleshooting will appear in case of an error.

Managing a Webhook

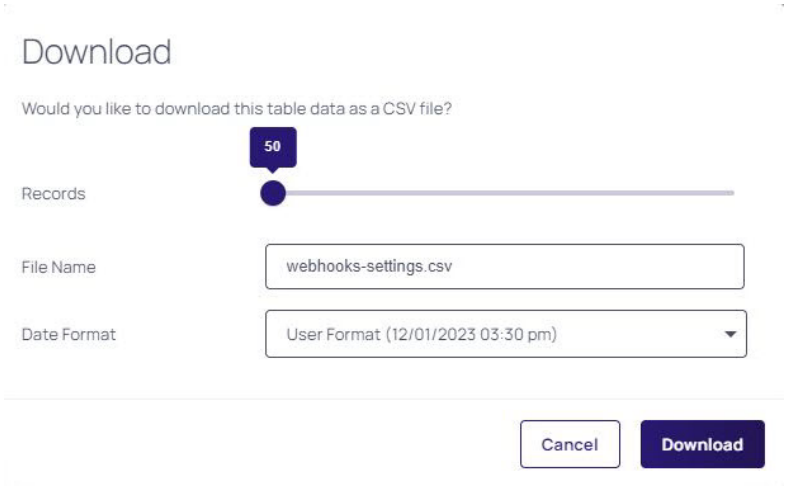
You can edit, enable, disable, or delete created webhooks in your Delinea Platform account.

You can also sort and filter existing webhooks, activate full-screen mode, or export all webhook records by selecting these icons in the upper right corner of the Webhooks page.



To export webhook records as a CSV file:

1. On the Webhooks page, click the **Download** icon.
2. Move the **Records** toggle to select the necessary number of records.
3. Provide the name for a file. Note that .csv format is supported only.
4. Select the appropriate date format.
5. Click **Download**.



Integrating Azure Sentinel

Azure Sentinel is a cloud-native security management solution running in the Azure cloud. You can integrate Azure Sentinel with the Delinea Platform with webhooks.

Prerequisites

Ensure you have all required accounts and utilities before starting the integration:

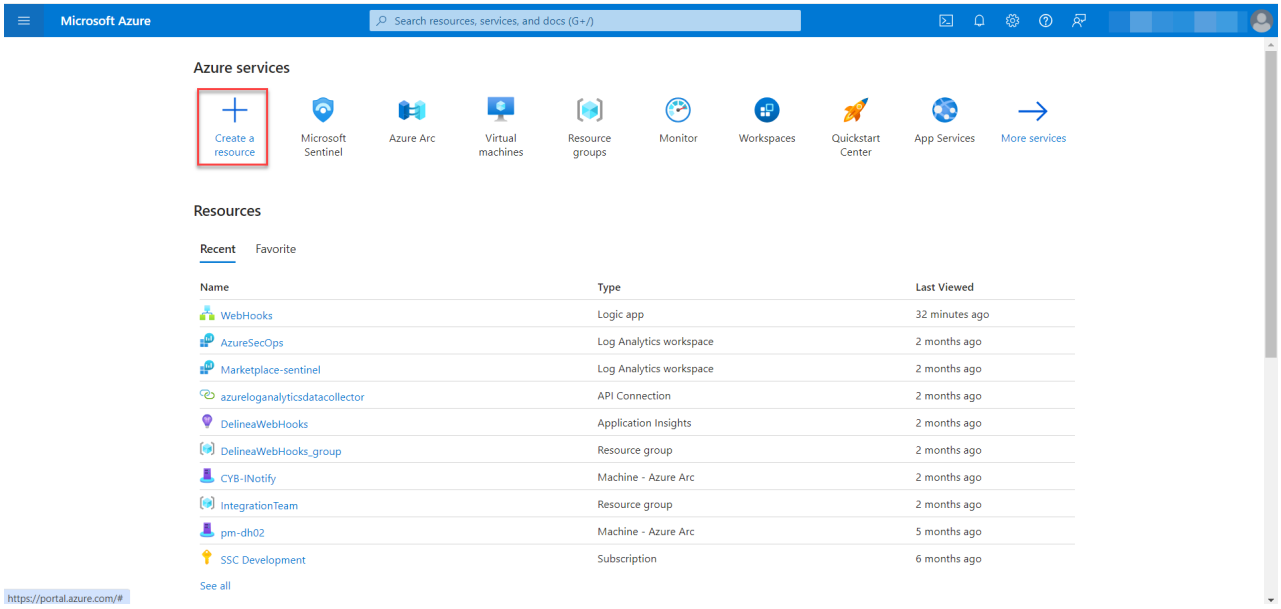
- Admin account on the Delinea Platform
- An Azure subscription
- Access to the Azure Portal
- A Log Analytics workspace

Configuring Azure Sentinel

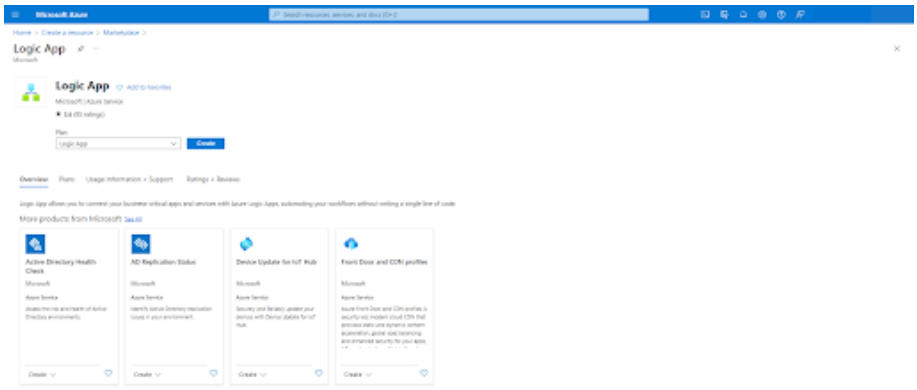
Azure Sentinel configuration requires creating a Logic app and setting up Azure Log Analytics.

Creating a Logic App in Azure

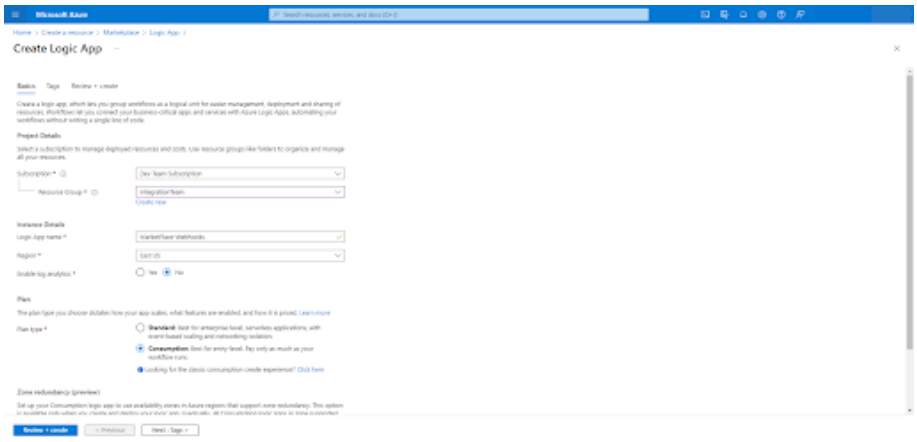
1. Log in to the Azure dashboard.
2. In the Azure services section, click **Create a resource**.



3. Search for the "Logic App" and select it.
4. Click **Create**.



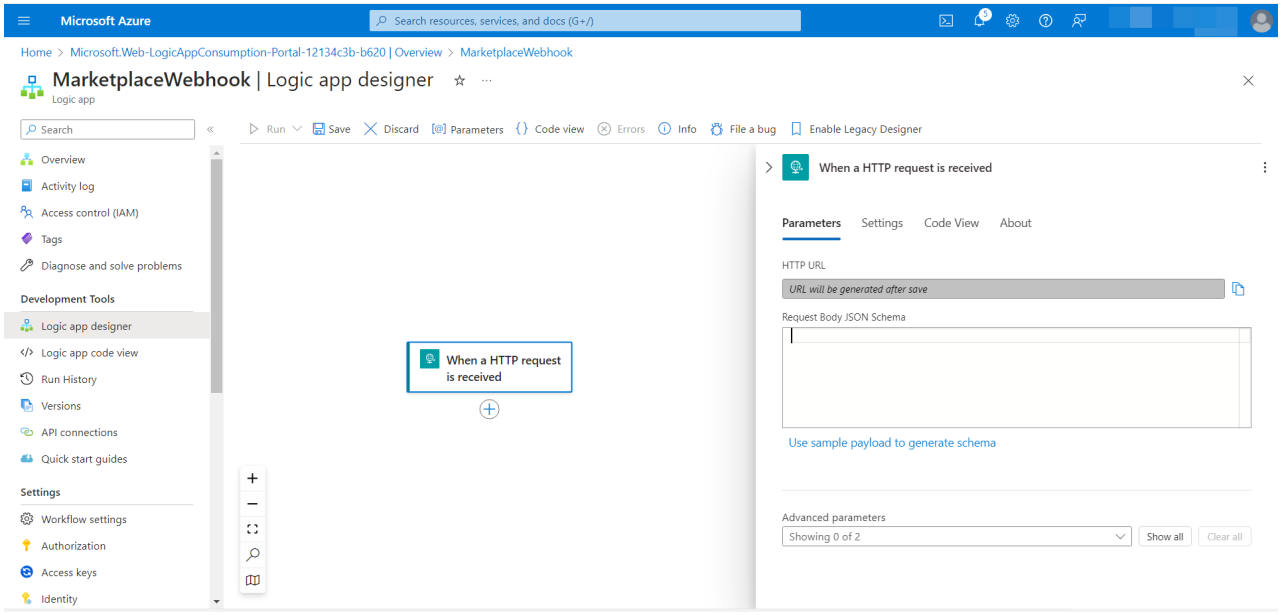
5. Fill in the required information for your Logic App and click **Review+Create**.



Once the deployment is done, your Logic App is created in Azure.

Setting up Azure Log Analytics

1. Click **Logic App Designer** under the "Development Tools" section in the Logic App.
2. In the designer, click **Add trigger**.
3. In the Add trigger window, search for "HTTP" and select "When an HTTP request is received." You will use this trigger when setting up a webhook on the Delinea Platform afterward.



4. Click **Use sample payload to generate schema** and paste the sample into the field.

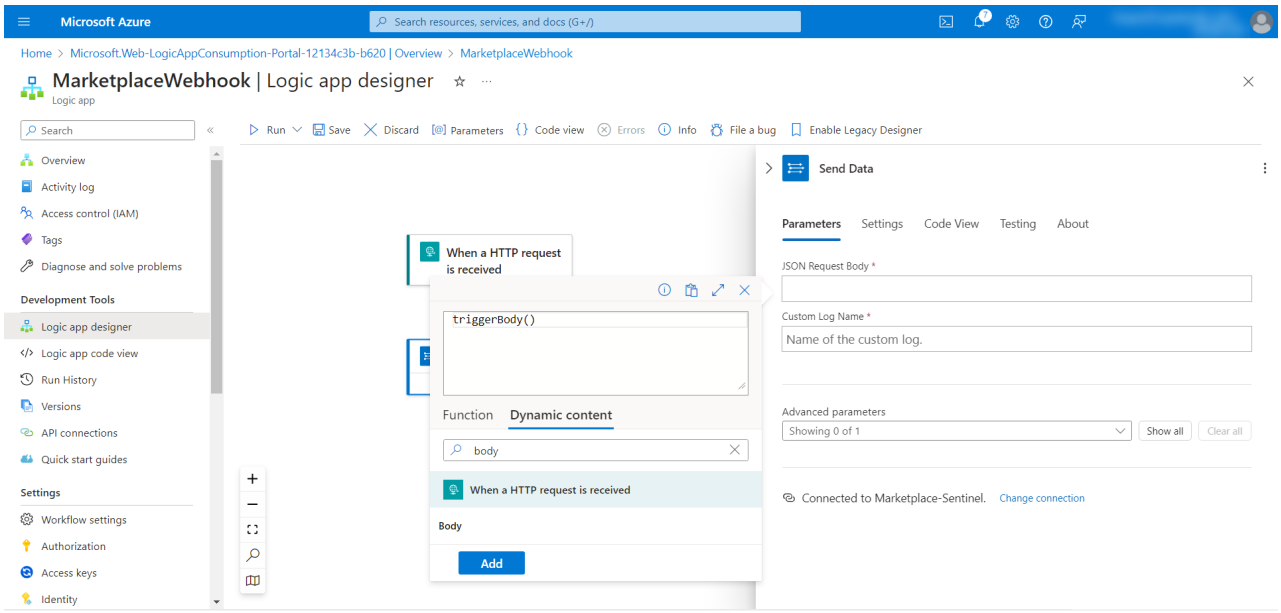
   Sample Payload

```
{
    "AuditEventMessageId": "87b928df-ccc5-46ed-8cc5-b2e88866a2b5",
    "TenantId": "7968fc7c-9205-4bd8-ad41-1432ffb8f7d3",
    "Service": {
        "Type": "permission"
    },
    "SessionId": "8194b39f-f7b6-4fb7-9876-2063ac5d3f00",
    "Source": {
        "Host": {
            "Network": {
                "AddressType": "ipaddress",
                "IpAddress": "0.0.0.0"
            }
        }
    },
    "Actor": {
        "Id": "9c52b7d1-863d-4de6-87ac-cf6c828fdd9f",
        "PlatformId": "9c52b7d1-863d-4de6-87ac-cf6c828fdd9f",
        "IdType": "platformid",
        "Type": "user",
        "Name": "user@tenant"
    },
    "Target": {
        "Host": {},
        "Id": "a08d7900-e5fd-49e4-bf29-f711b5d83825",
        "IdType": "platformid",
        "Type": "role",
```

```
            "Name": "Platform Admin"
        },
        "Action": {
            "Name": "Delinea.Permission.Data.Models.AssignedRole_Deleted",
            "Verb": "AssignedRole_Deleted",
            "TargetType": "Delinea.Permission.Data.Models"
        },
        "EventDateTime": "2023-09-21T14:13:57.7922228+00:00",
        "ProcessedTime": "0001-01-01T00:00:00+00:00",
        "Notes": "Role Platform Admin Deleted from RoleMembership a08d7900-e5fd-49e4-bf29-
    f711b5d83825.\n",
        "Tags": {},
        "AdditionalAttributes": {},
        "Level": 0,
        "UniqueConsumableId": "76ce017a-8538-453f-81d2-8d5b03816144",
        "Version": 0,
        "Redelivered": false,
        "RelayEvenIfExpired": false,
        "ParentCorrelationId": "00000000-0000-0000-0000-000000000000",
        "CorrelationId": "00000000-0000-0000-0000-000000000000",
        "TenantSecondaryId": "00000000-0000-0000-0000-000000000000",
        "ForceCompress": false
    }
```


Note: You can also take the schema payload from the Marketplace >Test webhook Request body. For details, see Testing a webhook.

5. Add a new action by searching for "Azure Log Analytics" and selecting "Send Data."
6. Add the body by clicking **Add** in the “Send data action” under Parameters.
7. Click inside the **JSON Request Body** field.
8. In the displayed dialog window, select **Dynamic content** tab.
9. In the search field, specify “body“ and click **Add**.
10. In the **Custom Log Name** field, provide the name for the table (the suggested name is *MarketPlaceEvent*).



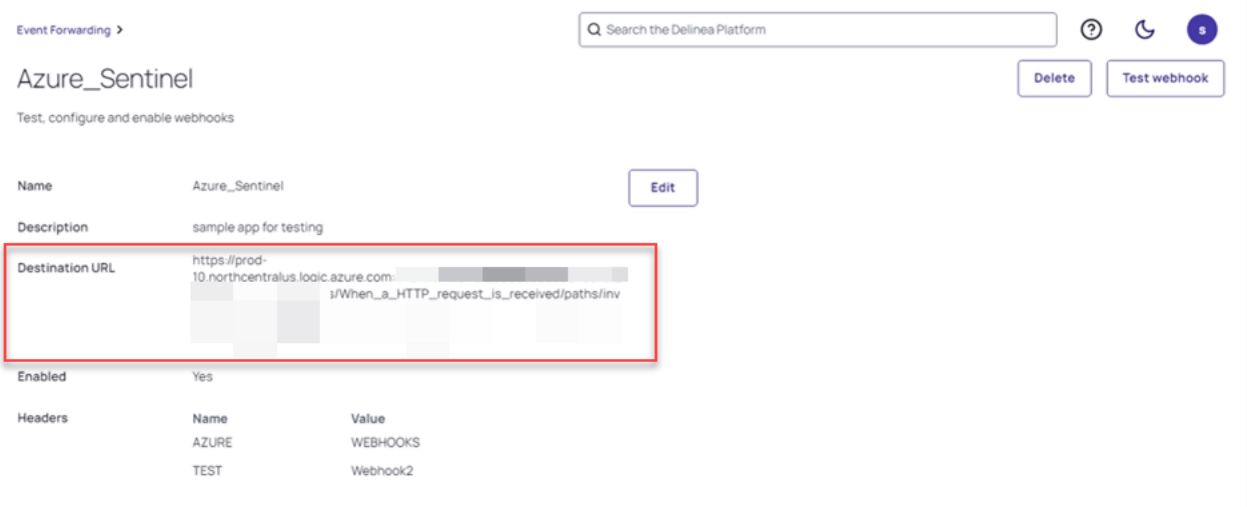
11. Connect to your Log Analytics workspace by providing the necessary credentials (Workspace ID, Shared Key).
12. Save the changes.

To get the WorkspaceID and Shared Key:

1. In the Azure portal, open your workspace
2. Click **Agents** under “Settings”
3. Click the arrow icon to expand the Log Analytics agent instructions.

Integrating Webhooks and Azure Sentinel

1. Log in to the Delinea Platform and go to **Settings** > **General Setup**.
2. On the Webhooks page, click **Create Webhook**.
3. In the **Destination URL** field, enter the HTTP request URL—an HTTP trigger configured in the Logic App.

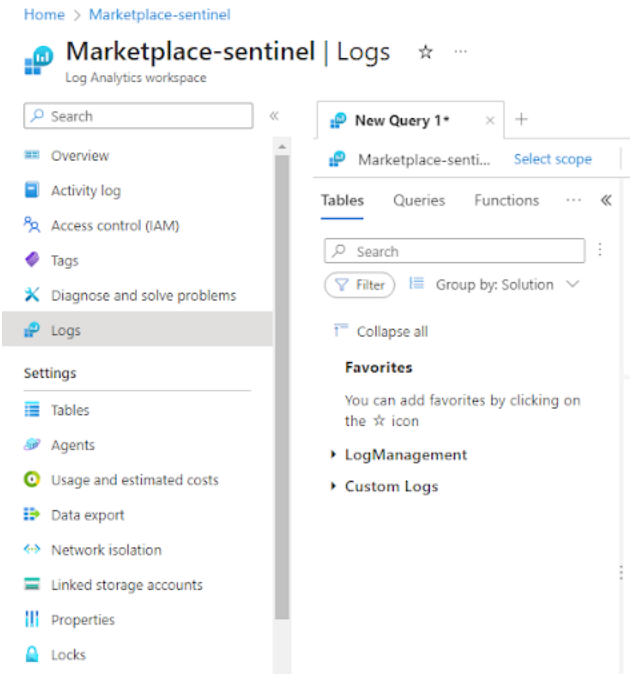


4. Click **Save**.
5. Verify the configured webhook on the Delinea Platform. For instructions, see Testing a webhook.

Verifying Logs for the Azure Sentinel Webhook

After you have set the integration, you should verify 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.
3. Click on the activity log and verify that logs from the Delinea Platform are triggered automatically.
4. Go to the Azure Sentinel dashboard in the Azure Portal.
5. In the left menu, click **Logs**.



6. Enter the following KQL query in the query editor: `MarketPlaceEvents_CL | take10`.
7. Verify that the log is displayed.

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 webhooks.

Prerequisites

Ensure you have all 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

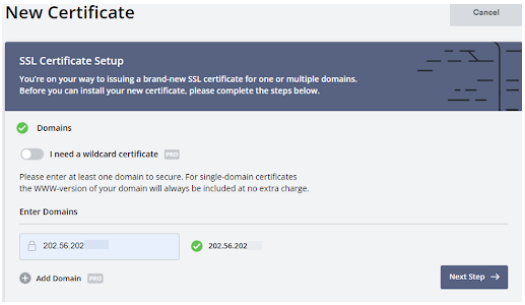
Setting up Splunk Enterprise

Splunk Enterprise configuration requires creating an SSL certificate and generating 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.

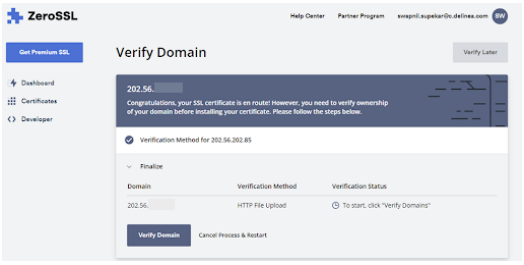
Creating a Certificate in Zero SSL

Below are the instructions on creating an SSL certificate issued by Zero SSL, but you can create an SSL certificate from any other certificate provider.

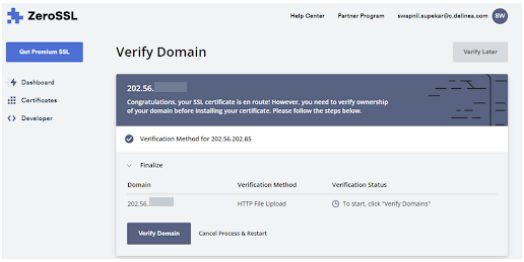
1. Go to Zero SSL > **Certificates** panel.
2. Click **New Certificate**.
3. Provide a valid domain for the certificate and click **Next Step** until you get the Verify Domain dialog box.



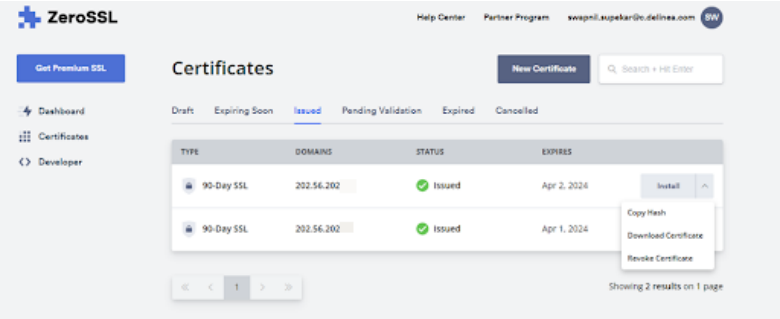
4. In the **Verify Domain** dialog box, select an **HTTP File Upload** and follow the instructions.



5. Click **Next Step**.
6. In the Verify Domain dialog box, check the details for the certificate verification and click **Verify Domain**.



7. Once done, go to the **Certificates** panel, select your certificate, and download it.

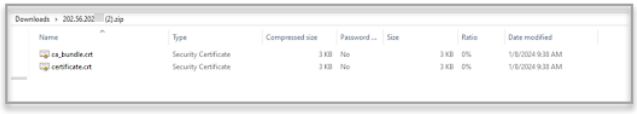


Configuring a Certificate in OpenSSL

Certificate configuration requires generating private key (`private.pem`), caCertificateFile (`certificate.pem`), and full chain (`full_chain.pem`) files.

Generating a Private Key

1. Copy the downloaded certificate to the Splunk directory on your local computer. An example of the folder path: `C:/programfiles/Splunk/etc/auth/sloccerts`



2. Check 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.

5. Run the `openssl genkey -algorithm RSA - out private.key` command to generate a 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`, you should first create a `Certificate Signing Request (CSR)` and then self-sign it. Open a terminal or a Command prompt and run the following commands:

- `openssl req -new -key ca_private_key.pem -out ca_csr.pem` to generate a Certificate Signing Request (CSR)

  This command generates a `Certificate Signing Request (CSR)` using the `private key ca_private_key.pem` and saves it to `ca_csr.pem`.

- `openssl x509 -req -days 365 -in ca_csr.pem -signkey ca_private_key.pem -out ca_certificate.pem` to self-sign a `Certificate Signing Request (CSR)`.

Generating a full_chain.pem file

Creation of 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:

1. In the Splunk directory on your computer, run the `cat your_certificate.crt intermediate.crt private.key > full_chain.pem` command to create a `full_chain.pem` file.
2. Replace `your certificate.crt` with the actual name of your SSL/TLS certificate file, `intermediate.crt` with the name of any intermediate certificate file (if applicable), and `private.key` with the name of your private key file.
3. Ensure you concatenate the files correctly: certificate, intermediate certificate(s), and then, the private key. The resulting `full_chain.pem` file should contain all the necessary information in the correct order.

   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.
4. Go to the Splunk directory on your local computer.
5. Open the `inputs.conf` file and specify the following data:

   ```
   [http]
   disabled = 0
   index = main
   enableSSL = 1
   port = 443
   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
   sslPassword = $7$jFSokSHgiIkooOG3Mq+38dYL1CYRU1OLwdzPlnXnPOpsJ/R5+B/
   db17Z
   ```

6. Open the `web.conf` file and specify the following data:

   ```
   [settings]
   enableSplunkWebSSL = true
   httpport = 8443
   ```

```
enableSplunkWebSSLDebug = true
```

7. Restart your Splunk server.

Integrating Webhooks and Splunk Enterprise

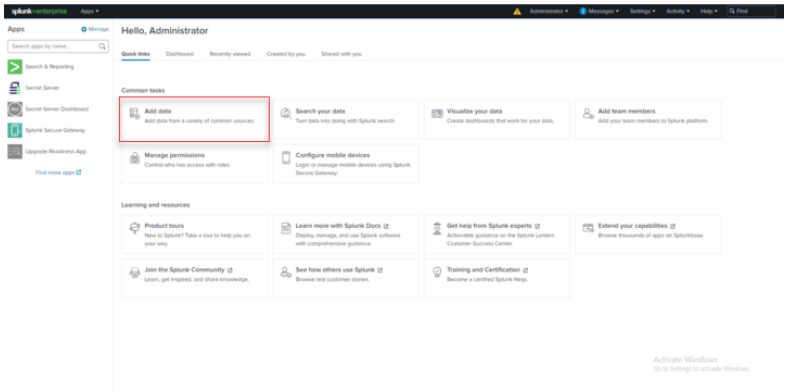
After you have generated and managed certificates, setting up integration between Splunk Enterprise and Delinea Platform webhooks is available.

Configuring Splunk Enterprise HTTP Event Collector

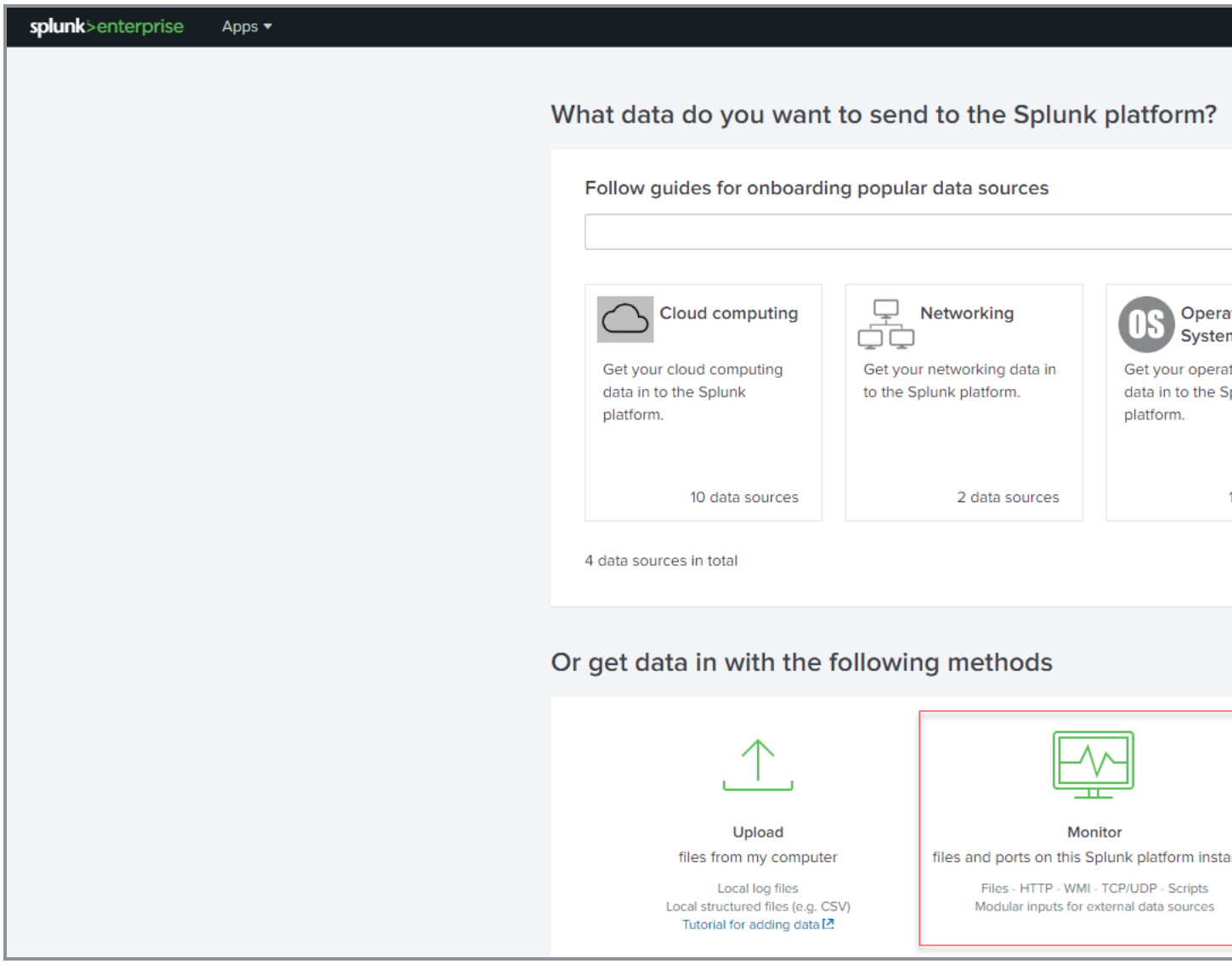
1. Install a Docker container to run Splunk Enterprise inside it. For information on Docker container installation, see the Splunk Enterprise official documentation.
2. Open a Docker container and run Splunk Enterprise with an extra port exposed for HTTP Event Collector (HEC) using the following command:

   ```
   docker run -d -p 8000:8000 -p 8088:8088 -e SPLUNK_START_ARGS='--accept-license' -e SPLUNK_PASSWORD='Test789!' splunk/splunk:latest
   ```

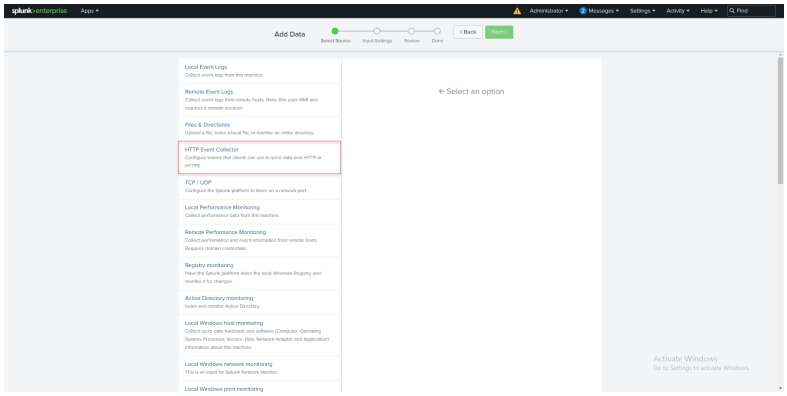
3. Log in to your Splunk Enterprise account with admin permissions.
4. On the **Quick links** tab, click **Add Data**.



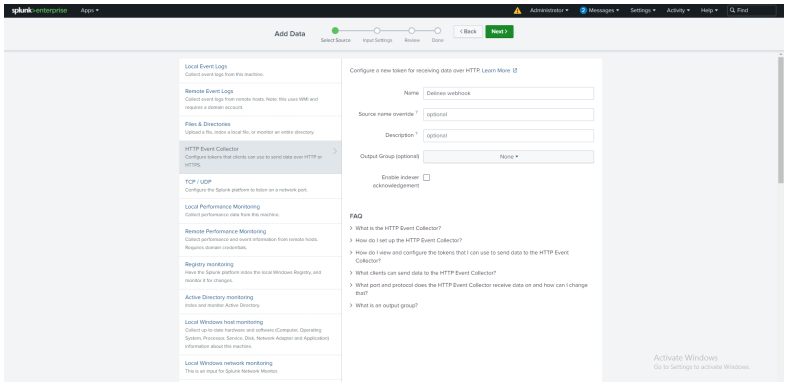
5. Next, click **Monitor**.



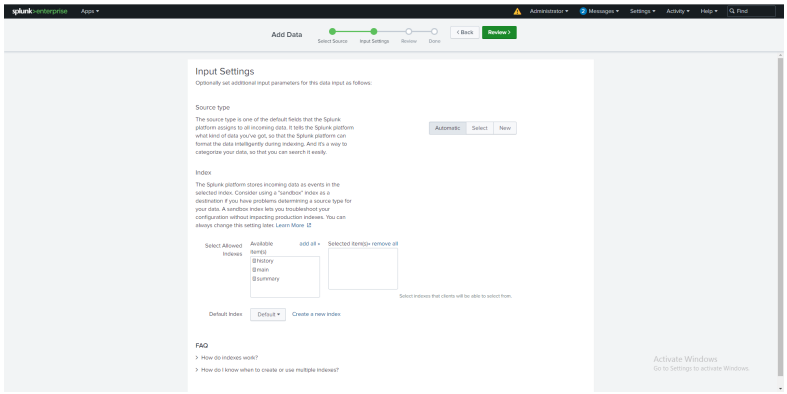
6. From the displayed left-side panel, select **HTTP Event Collector**.



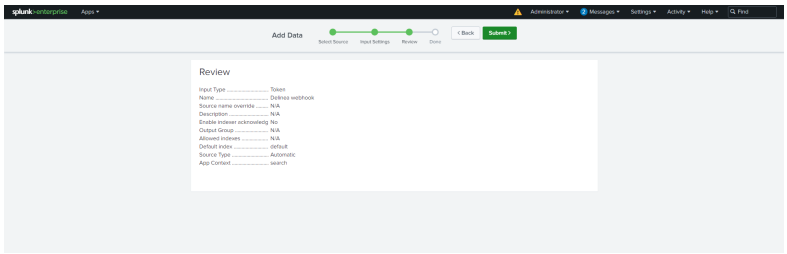
7. In the HTTP Event Connector form, specify the required details and click **Next**.



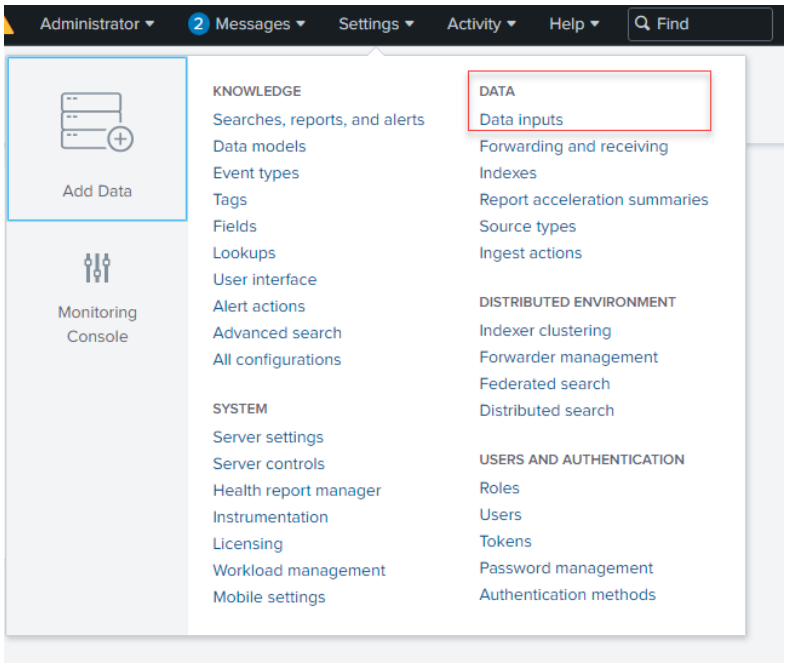
8. Click **Next**, check the displayed details, and click **Review**.



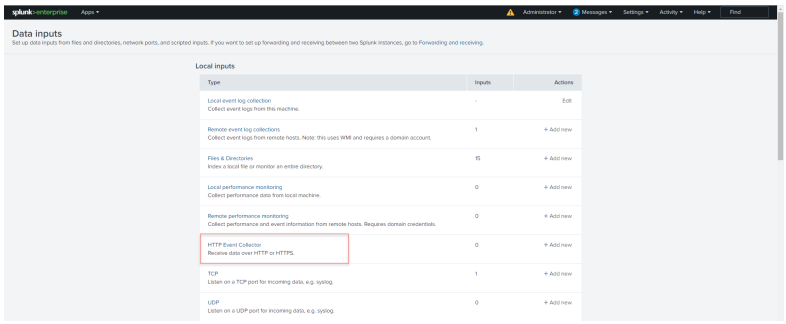
9. Click **Submit**.



10. Go to **Settings** > **Add Data** > **Data inputs**.

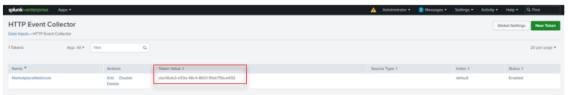


11. In the Data inputs dialog box, click **HTTP Event Collector**.



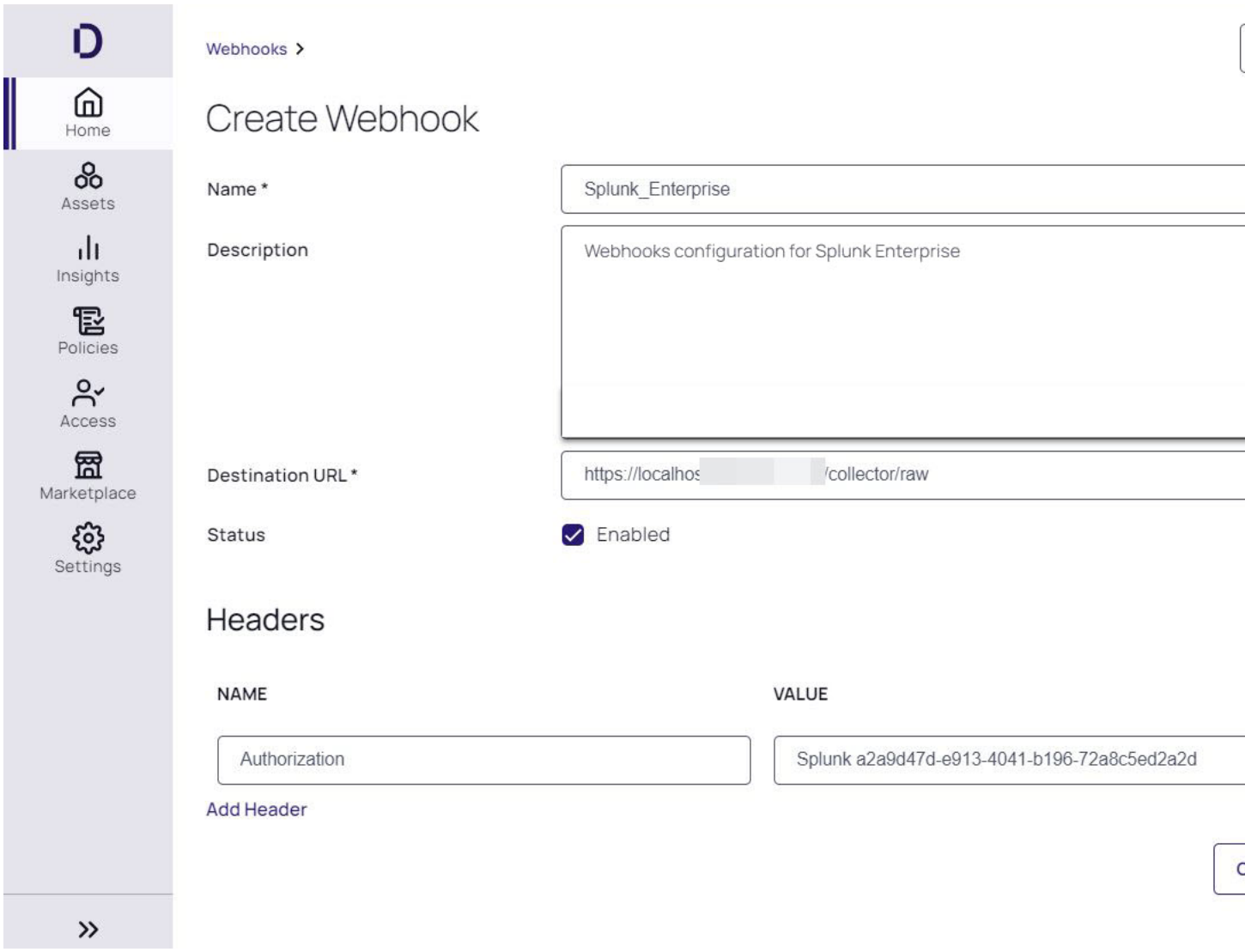
12. In the HTTP Event Collector dialog box, copy a **Token Value**.

    This Token Value you will use during a webhook creation in the Delinea Platform.



Creating Webhooks for Splunk Enterprise

1. Log in to the Delinea Platform.
2. Click **Settings** from the left navigation.
3. Click **Webhooks** under **General Setup**.
4. On the Webhooks page, click **Create Webhook**.
5. Specify necessary details, and in the **Value** field, enter the Token Value created for HTTP Event Connector in Splunk Enterprise.



6. Click **Save**.
7. Verify the configured webhook on the Delinea Platform. For instructions, see Testing a webhook.

Troubleshooting

Issue:

An SSL error as a result of the webhook test.

Solution:

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:

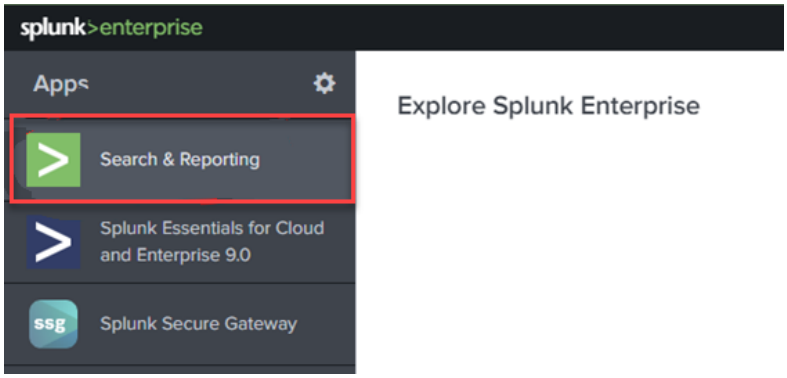
```
var handler = new HttpClientHandler
{
ClientCertificateOptions = ClientCertificateOption.Manual,
ServerCertificateCustomValidationCallback =
(httpRequestMessage, cert, cetChain, policyErrors) => true
};
```

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

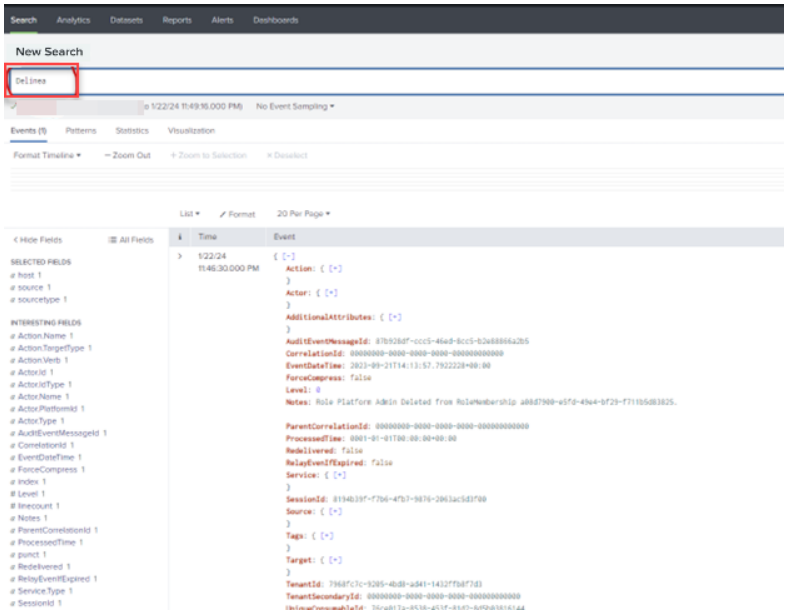
When you have ensured that webhooks are correctly configured for Splunk Enterprise, you can check logs received via webhooks.

1. Log in to your Splunk Enterprise account with admin permissions.
2. From the **Apps**, select **Search & Reporting**.



3. In the **New Search** field, specify "Delinea" and press Enter key.

4. Verify that the log is displayed.



Managing Third-Party Contractors and Vendors

Important: This functionality is currently available only to customers participating in a private preview. If you'd like to participate to be among the first to try this functionality, ask our support or account team for details.

Organizations can use the membership-type capability 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	✓ (RAS)	✓
Request access to secrets	✓	✓
Approve access to secrets		✓
Share secrets		✓

Capability	Vendor User	IT User
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 that have purchased RAS concurrent user licenses, are entitled to Vendor User capabilities out of the box. Learn more about RAS "Entitlements and Licenses" on page 324.

Important: Entitlements are enforced even if a user is granted RBAC permissions for related actions.

Local Users

Customers can use their Platform local directory to onboard third-party users requiring short-term access, or when they do not want to add third-party users to their own identity sources. See "Adding Users" on page 186 for more details.

Bulk Import of Vendors

The bulk import process is useful for organizations that deal with large numbers of third-party users and need an efficient way to manage access to Secret Server entitlements. The bulk import process involves preparing a file with user data, formatting it according to the system's requirements, and then uploading it through a specific interface provided by the system.

For more detailed information about importing vendors in bulk, please refer to "Bulk Import Local User Accounts" on page 188.

Federated Vendors

Tenant administrators will need to create a custom attribute in the identity provider (IdP) and map it to a *PlatformUserMembershipType* claim in the Delinea Platform. Claims for users need to have a value of either **Vendor** or **Employee**.

For more information about managing third-parties from a federated identity source using SAML or OIDC, please refer to the "Federation" on page 50 documentation of the Delinea Platform.

Privilege Control for Servers

While the Delinea Platform provides Privileged Access Management (PAM) protecting your organization's privacy, secrets, and resources at the network level, Privileged Control for Servers (PCS) drives those capabilities all the way down into the individual server and computer endpoints in your corporate network. PCS is supported by some new broader platform services introduced around the same time as PCS, and these services are briefly described below.

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, it essentially becomes an Active Directory client and 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 fail-over 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 into and performing elevated actions on remote computers and servers managed by the Delinea Platform. 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 into 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.

Audit Collector

Delinea Audit Collectors transmit machine-level audit data to the Delinea Platform, allowing recorded activities and events to be presented, examined, and preserved. They 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 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 collectors to ensure uninterrupted auditing. Additional collectors can be deployed at any point for additional resiliency or improved scale.

Command Relay

Command Relay facilitates communication between the Delinea Platform and the customer 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.

We expect that most Privilege Control for Servers (PCS) customers will be existing Delinea clients, with standard environments and components already deployed for the Delinea Platform and Secret Server.

Note: PCS does not support FIDO2 MFA

PCS End-to-End Installation and Run Guide

This feature is currently available only to customers participating in our public preview. If you'd like to participate and be among the first to try this feature, ask our support or account team for details.

Assumptions

This guide assumes that you already have the Delinea Platform set up for fundamental tasks and that you understand how to use them:

- Platform and Secret Server integration
- Discovery for active directory users and servers
- Setting up a site for engines
- Setting up a RAS engine
- Installing the Delinea Connector
- Vaulting an account

Overview

Setting up Privileged Control for Servers to work on the platform and your network servers involves the following tasks:

1. "Setting Up PCS Service Accounts" below
2. "Enable IWA Service on Connectors" on the next page
3. "Installing the Delinea Engine on Managed Servers " on page 430
4. "Installing the Delinea Agent on Managed Servers" on page 432
5. "Setting up PCS Profiles " on page 436
6. "Setting up PCS Policies" on page 437
7. "Setting up Audit and Session Recording" on page 441
8. "Setting up Use My Account for *nix Systems" on page 442

Configuring Firewall Ports for PCS

To use Privilege Control for Servers, configure firewall ports appropriately according to the two resources below:

- "Platform Architecture and Topology" on page 14
- "Delinea Engine Management" on page 252

After you configure the firewall ports correctly, return to this page and pick up reading again in the section below.

Setting Up PCS Service Accounts

On the platform, you need to create two domain service accounts with roles and permissions that are specific to PCS. These accounts must be placed in the Secret Server vault to be used for setting up Delinea Engine Management and its Command Relay workload. You must create at least one of each of these accounts but you can also create more according to best practices for the Secret Server Discovery and Directory Services.

- **Delinea Engine Management Admin**
  See Engine Management Account Permissions and Roles
- **Delinea Command Relay Admin**
  See Command Relay Account Permissions

Also see Delinea Engine and Engine Management and Roles and Permissions.

Installing 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 at The Delinea Connector and in these subsections:

- Requirements
- Recommendations
- Permissions Required for Alternate Accounts and Organizational Units
- Platform: Download the Delinea Connector and Get a Registration Code
- Servers: Install and Configure the Delinea Connector

- Servers: Enable Auto-update for the Delinea Connector
- Ping Connector

After you successfully install the Delinea Connector, return to this page and pick up reading again in the section below.

Enable IWA Service on Connectors

Enable Integrated Windows Authentication for PCS by following the procedures at IWA Configuration.

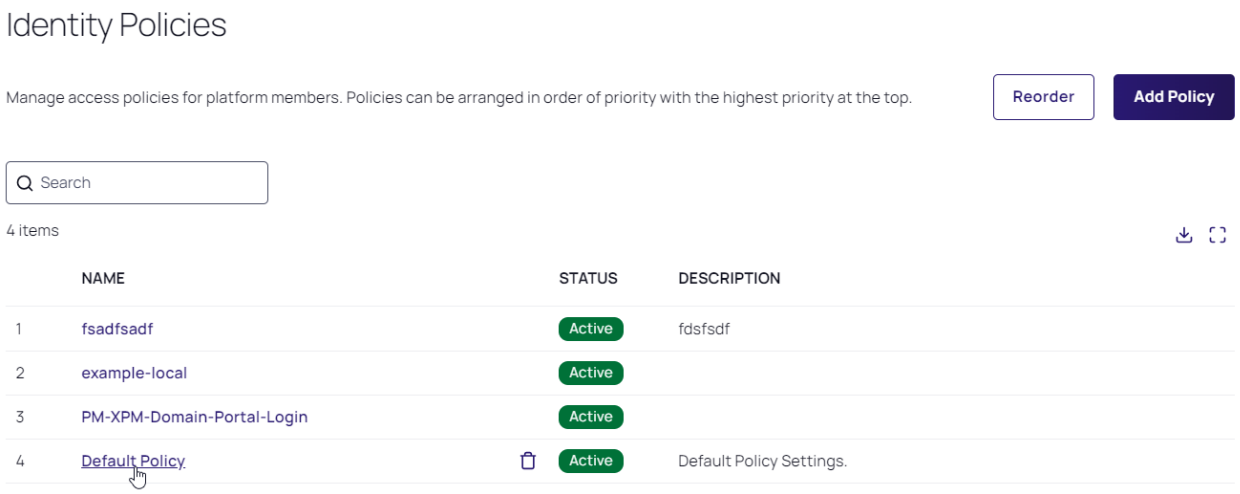
The Delinea Platform enables you to accept Integrated Windows Authentication (IWA) as sufficient authentication for Active Directory user accounts to log in to the platform. The platform uses Kerberos SSO for authentication. With IWA enabled, the browser uses the current user's Active Directory information to prove its knowledge of the password through a cryptographic exchange with the in-process web server built into the connector.

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.

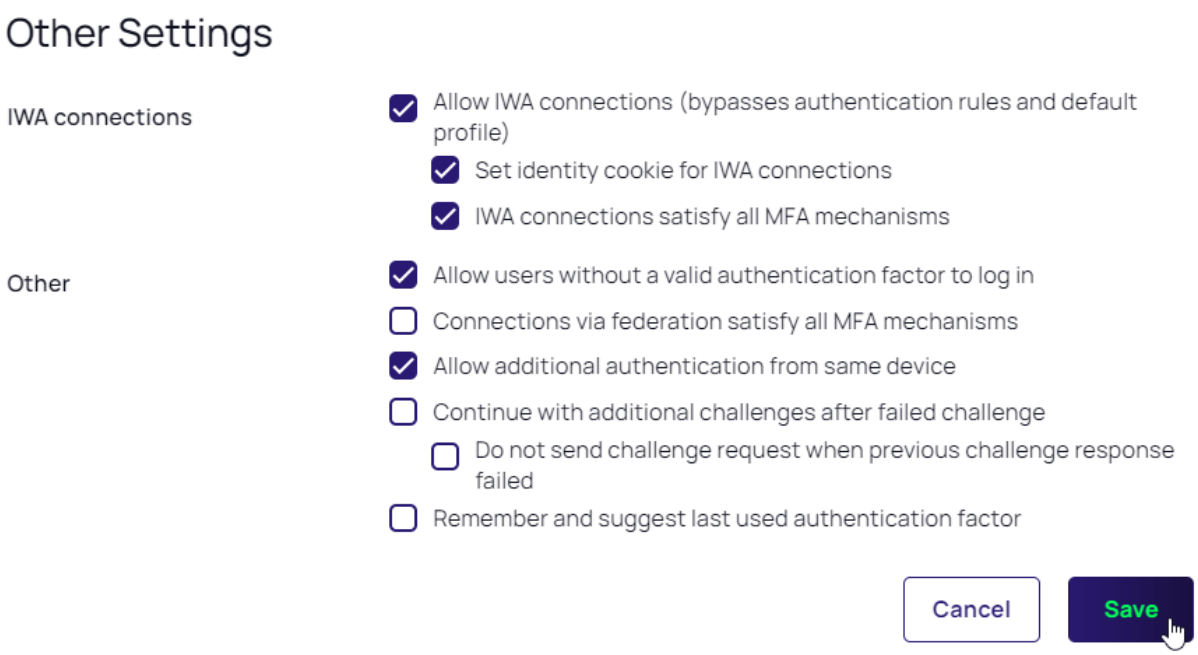
Allowing IWA Connections for All Users in the Default Policy

1. Click **Access** from the left navigation menu, then click **Identity policies** from the secondary menu.
2. Click to open the **Default Policy**.



3. Select the **Authentication** tab.

4. Scroll to the Other Settings section and click **Edit**.



5. Confirm that all three options for IWA connections are selected:
   - **Allow IWA connections** (bypasses authentication rules and default profile): Enabled by default. Configures the platform to bypass already-configured authentication rules and default authentication profiles when IWA is configured.
     - **Set Identity Cookie for IWA Connections:** 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:** This option tells the platform to allow IWA to override all application specific authentication requirements.
6. Log in to the Delinea Platform as one of the AD users you created for testing purposes.
7. After you successfully ensure that IWA connections are allowed for all users, return to this page and pick up reading again in the section below.

Obtaining an IWA Connector 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 conveniently download the public key certificate when needed. You can obtain an IWA Connector Host Certificate using any of the following processes:

- Obtain a certificate from a trusted external certificate authority (CA) such as Symantec or GoDaddy.
- 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.

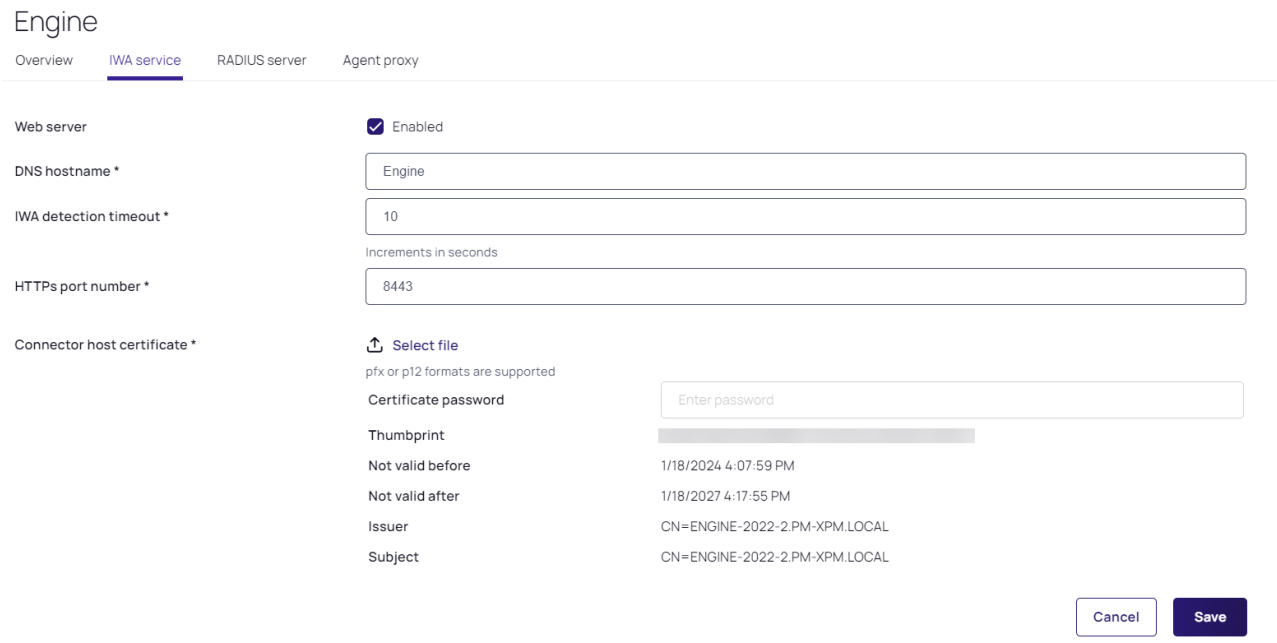
- Generate a self-signed certificate, which would require trusting it on each endpoint it is used on (or through other policy/management infrastructure).

To Generate a self-signed IWA connector host certificate for Agent Installation

1. Run the script below as an administrator on the server running the 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
```

1. Click **Settings** from the left navigation, 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. Enter the information for **DNS hostname** and **IWA detection timeout**.

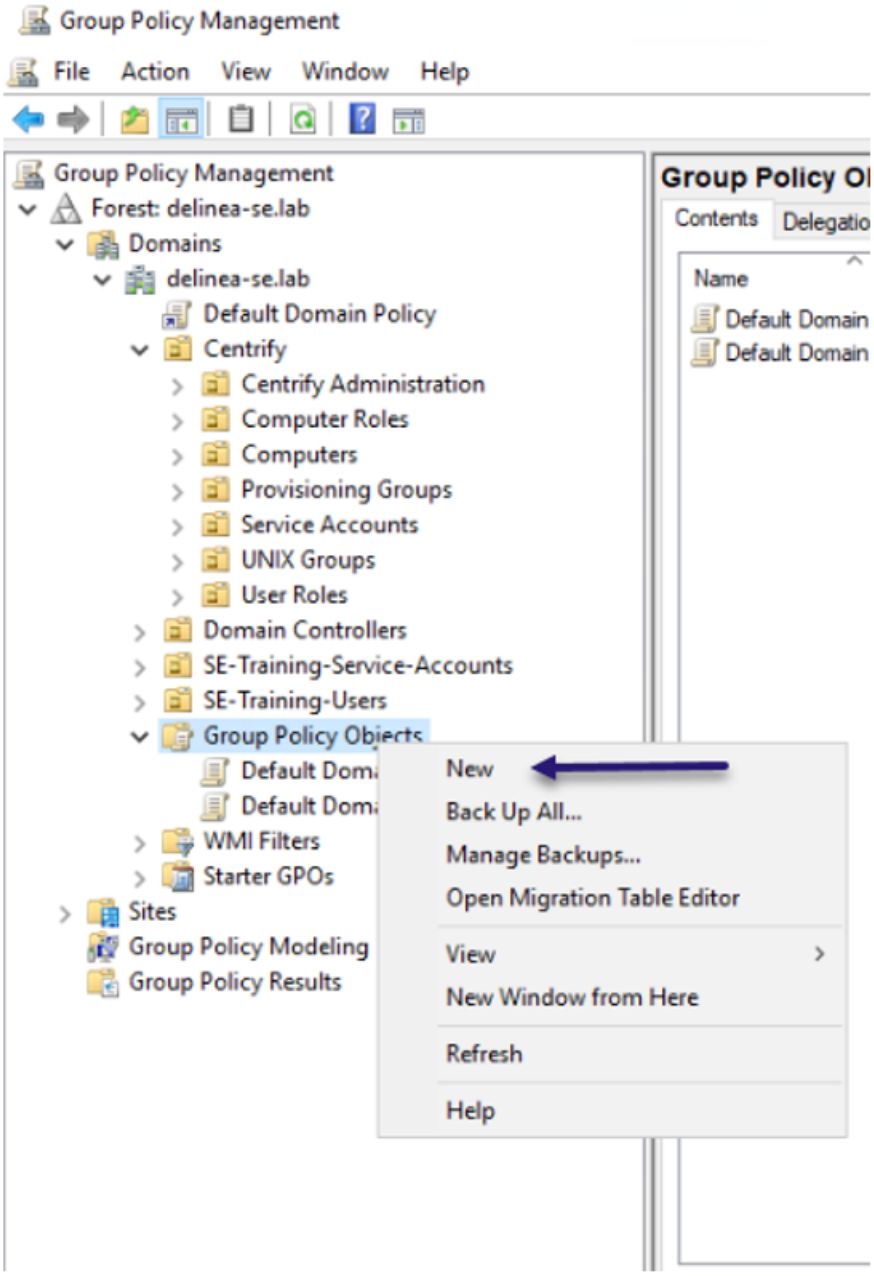
6. In the **HTTPS port number** field, enter **8443**. For MFA on PCS, endpoints that need to do MFA must be able to contact the Connector on 8443 and 8080.
7. Next to *Connector host certificate*, click **Select file.**
8. Browse to and select the host certificate file (.pfx or .p12 formats are supported) to upload it.
9. Select **Open**.
10. Enter the password for the certificate. The password is the one you entered when running the PowerShell script to generate the certificate.
11. Click **Save**.
12. Click **Edit** again.
13. Next to Web Server, select **Enabled**.
14. Click **Save**.
15. Next to Connector host certificate, click **Select File**.
16. Upload the Connector host certificate.
17. Enter the password you used when running the PowerShell script to generate the certificate.

Download the Connector Host Certificate

1. Click the **IWA service** tab and click **Download** at the lower right to download the Connector host certificate.
2. Click the Agent Proxy tab and verify that the agent is enabled on the proxy server.

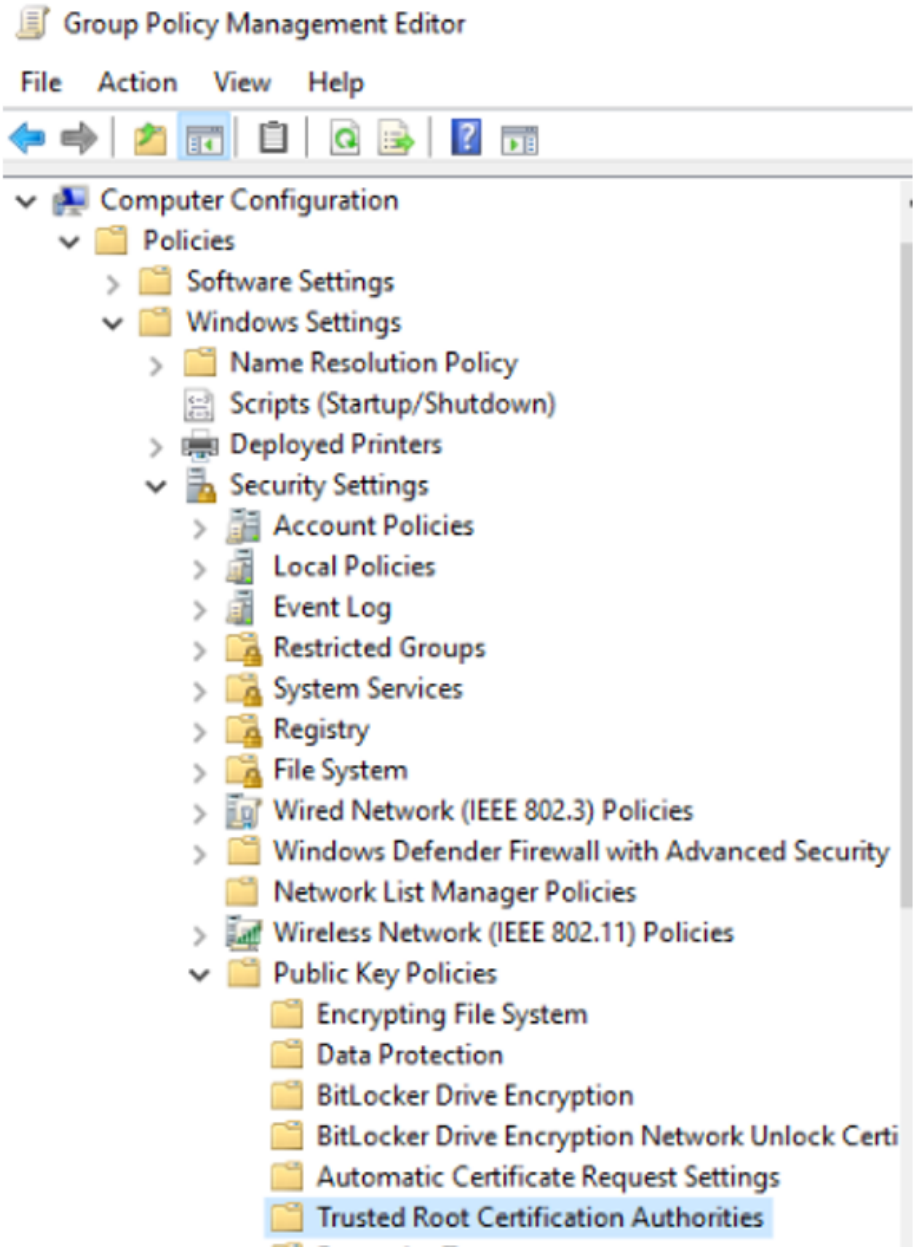
Distribute the Connector Host Certificate for Agent Installation

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:



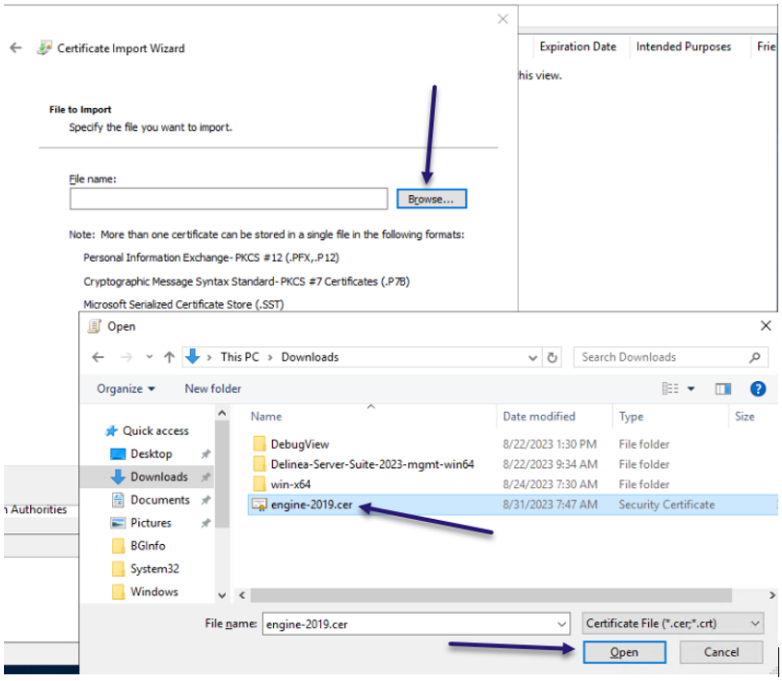
3. Expand the forest (ex. delinea-se.lab).
4. Expand the domain (ex. delinea-se.lab).
5. Right click **Group Policy Objects.**

6. Select **New**.
7. In the New GPO dialog, enter a name.
8. Click **OK**.
9. Right-click the name of the GPO you just created.
10. Select **Edit**.
11. On the host machine, open the **Group Policy Management Editor**.
12. Navigate by clicking the following: **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Public Key Policies** > **Trusted Root Certification Authorities**.

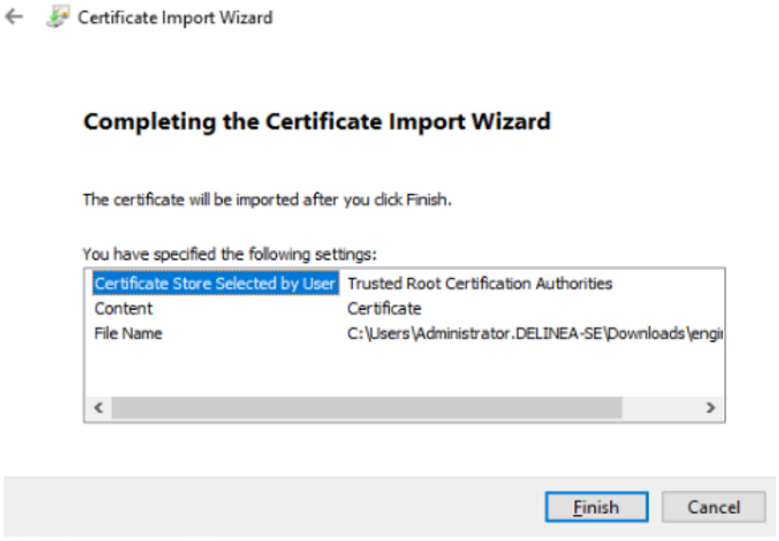


13. Right-click **Trusted Root Certification Authorities** and select **Import**. The Welcome screen opens to the Certificate Import Wizard.
14. Click **Next**.
15. For File to Import, select **Browse**.

16. Navigate to the host certificate you downloaded earlier.

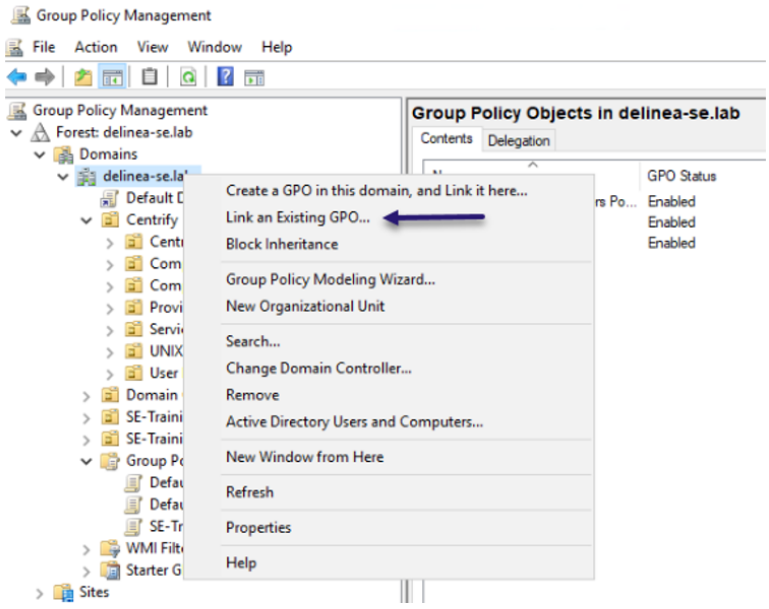


17. Click **Open**.
18. Click **Next**.
19. Next to *Certificate Store Selected by User*, you should see Trusted Root Certification Authorities.



20. Click **Next**.
21. Click **Finish**.
22. Wait for the Certificate Import Wizard pop-up.

23. Click **OK**.
24. Close the Group Policy Management Editor.
25. In Group Policy Management, right-click the domain you created.
26. Select **Link an Existing GPO...**



27. Select the IWA Host Certificate.
28. Click **OK**.

Installing the Delinea Engine on Managed Servers

Delinea Engine and Engine Management are components of the larger Delinea Platform product and they are requirements for using Privilege Control for Servers. The Delinea Engine runs two workloads for PCS:

- Command Relay
- Audit Collector

On the server where the Delinea 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. Install the Delinea Connector on your target servers by following the procedures at Delinea Engine and Engine Management and in these subsections:

- Solution Components
- Engine Management Account Permissions and Roles
- Engine Sites
- Engines
- "Managing Engines" on page 261

- Updating an Engine
- Uninstalling an Engine from the Platform
- Workloads
- Delinea Audit Collector Workload
- Command Relay Workload
- The DelineaZone

Updating the Engine Management Settings

1. Click **Settings**, then select **Sites and Engines**.
2. Select the site that you want to update using the vaulted secret you just created.
3. Click the **Settings** tab.
4. Click **Edit** next to Delinea Audit Collector.
5. Enter the following configurations:
   - Collector Port: **5063**
   - Session Recording: **enabled**
6. Click **Save**.
7. Click **Edit** next to Delinea Command Relay.
8. Next to Command Relay Domain Admin 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.**

Update the Engine

1. Click **Settings**, then select **Sites and Engines**.
2. Click the name of the site where your Delinea engine is installed.
3. Click the **Engines** tab.
4. Look at the Engine Version column.

If the version is not 1.2.33.0 or later, the engine must be updated as described below:

1. Click the name of the engine
2. Click the **Workloads** tab.
3. Look at the command-relay version column.
4. If the version is not 1.0.94 or higher, restart the Delinea engine Service on the server that is running the Delinea engine. Wait for Command Relay to update.
5. Log in to the server running the Delinea engine.

6. Open PowerShell as an administrator.
7. Copy the uninstall script below:

```
Clear-Host;Write-Host "Uninstalling Delinea Engine"; $ZipFile =
"$env:TEMP\DelineaEngineInstaller.zip"; $InstallerFolder = "$env:TEMP\$(New-Guid)";
$ProgramFilesFolder = 'C:\Program Files\Delinea Engine'; $ProgramDataFolder =
'C:\ProgramData\Delinea 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; }
```

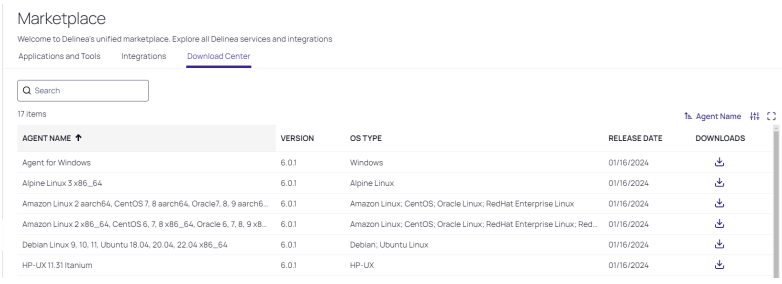
8. Paste the script into PowerShell.
9. Run the script.
   Note: If errors happen during the uninstall. Close the PowerShell windows. Relaunch PowerShell as administrator and rerun the uninstall script.
10. On the platform, click **Settings**, then click **Sites and Engines**.
11. Open the site where the Delinea engine is installed.
12. Click the **Engines** tab.
13. Click the engine name.
14. Click **Delete Engine**.

Installing the Delinea Agent on Managed Servers

Please see additional content at Agents Reference.

Download the Agent

1. Log in to your platform tenant.
2. Click **Marketplace** from the left navigation menu.
3. Click the Download Center tab.



4. In the Search box, enter **Agent**.

5. Find the agent for your OS.
6. Click the download icon.
7. Wait for the package to compile and download.

Install the Linux Agent

Requirements

- Perl
- Forward and Reverse DNS entries for each *nix Server

Note: If you require a different version of *nix agent please visit: `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.

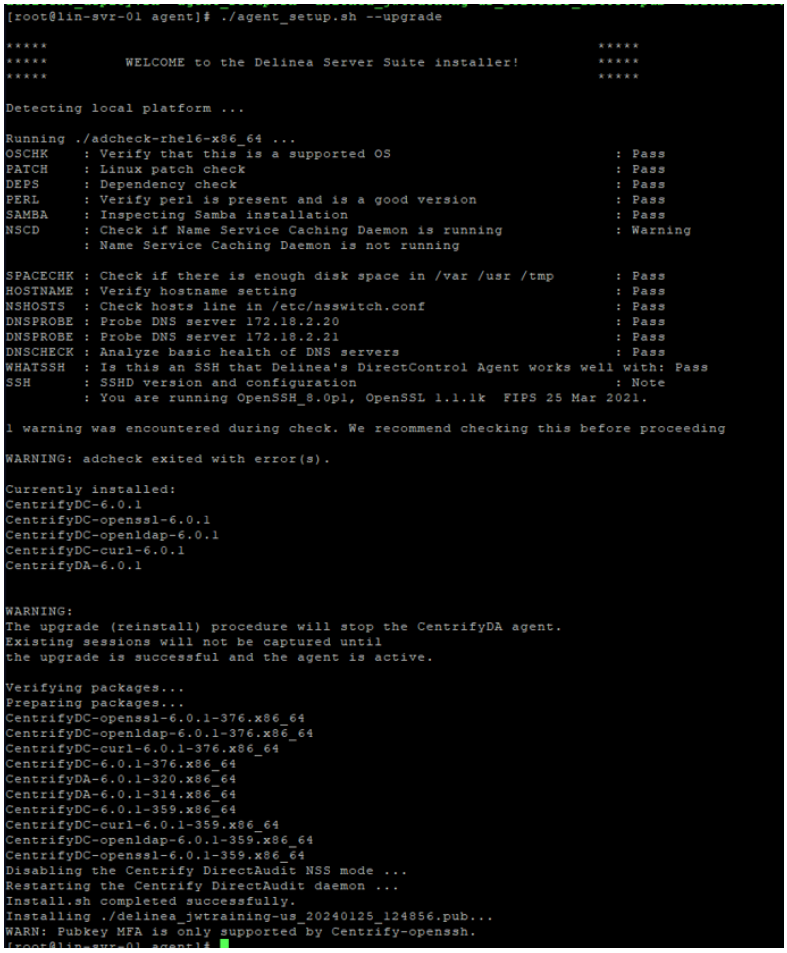
Upgrade the Linux Agent

1. Login to your Linux server.
2. Navigate to the folder that you created earlier.

```
[root@lin-svr-01 ~]# ls
agent_install.sh  anaconda-ks.cfg  delinea  delinea-agent
[root@lin-svr-01 ~]# cd delinea-agent/
```

3. Unzip the download package (e.g. unzip rhel-x86_64.zip)

4. ./agent_setup.sh --upgrade

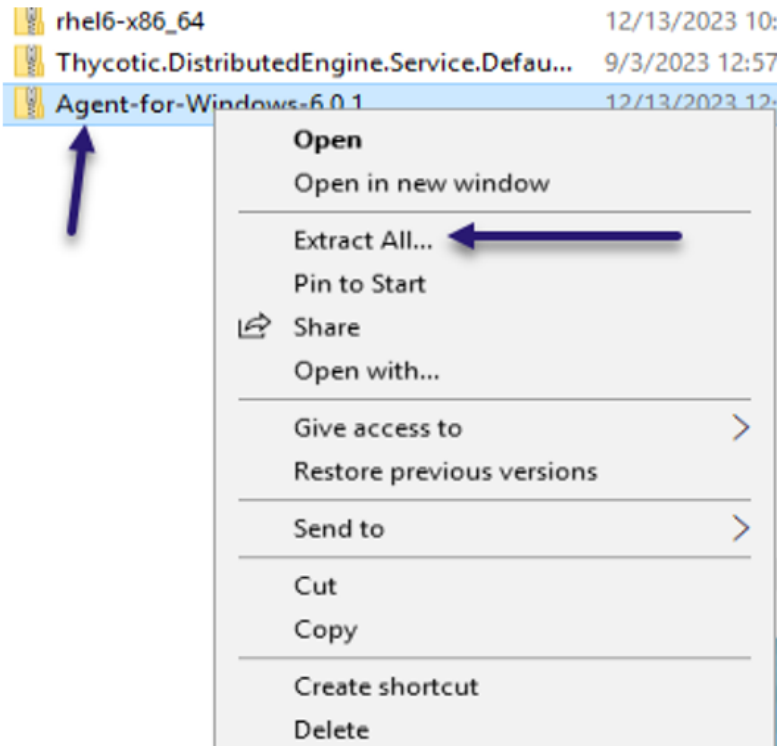


Install the Windows Agent

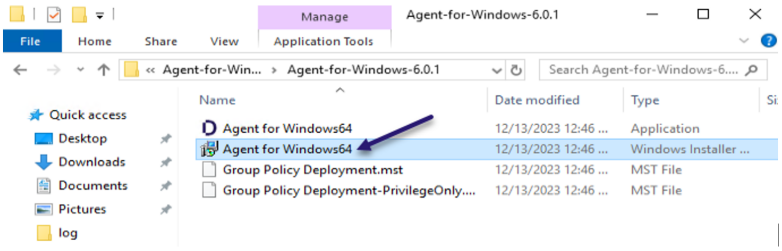
Requirements:

- .Net 4.8 is needed – already done in lab environment
- Must be joined to the AD domain and zone

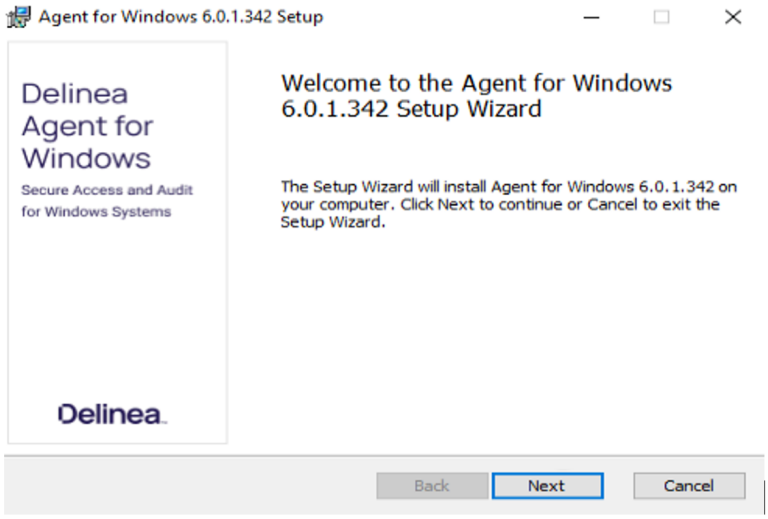
1. Log in to the server as domain administrator.
2. Select the Windows Agent you downloaded in the previous step.
3. Right-click the downloaded Windows zip agent file.
4. Select **Extract All...**



5. Click **Extract**. The extracted files will open in a new file explorer window.
   Note: The container package is in ZIP format, but the files inside are in TGZ format.
6. Open the **Agent-for-Windows-6...** folder.
7. Launch the agent for Windows 64.



8. Click **Next**. The Delinea Agent for Windows Wizard opens.



9. Click **Next**.
10. Accept the terms of the license agreement
11. Click **Next**.
12. Keep the default destination folder.
13. Click **Next**.
14. Click **Install**.
15. Select **Run Agent Configuration Wizard**

Agent Configuration Wizard

1. Click **Add Service**.
2. Click **Privilege Elevation Service**.
3. Click OK.
4. Select the **DelineaZone**.
5. Click **Next**.
6. Select **Yes** to add the Domain Admins.
7. Select **Yes to Restart.**

Setting up PCS Profiles

Note: For additional information on platform authentication profiles, see Identity MFA

Emergency Access Profiles

You do not need to create any profiles for Emergency Access policies, because their Rule Type is always Allow, meaning they do not accept a Rule Profile (Authentication Profile).

Endpoint Login Profiles

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, automatically.

Privilege Elevation Profiles

Profiles for Privilege Elevation policies should not have Challenge 1 set to Password, because the platform will always present a password challenge to the user first, automatically.

Setting up PCS Policies

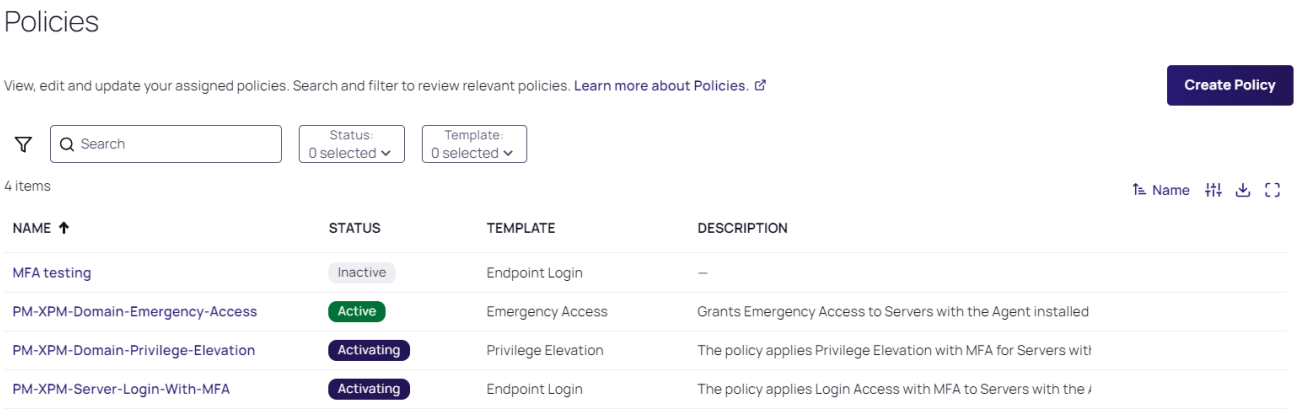
PCS authentication policies provide users with machine-level (server) permissions for logging into and performing actions on remote computers and servers managed by Delinea. By assigning machine-level policies, you can ensure that each asset adheres to compliance standards, maintaining both security 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.

View Policies

Click **Policies** from the left navigation menu. The Policies page opens, listing each policy available in your platform environment, and displaying each policy's **Name**, **Deployment Status**, base **Template**, and **Description**.

Deployment Status

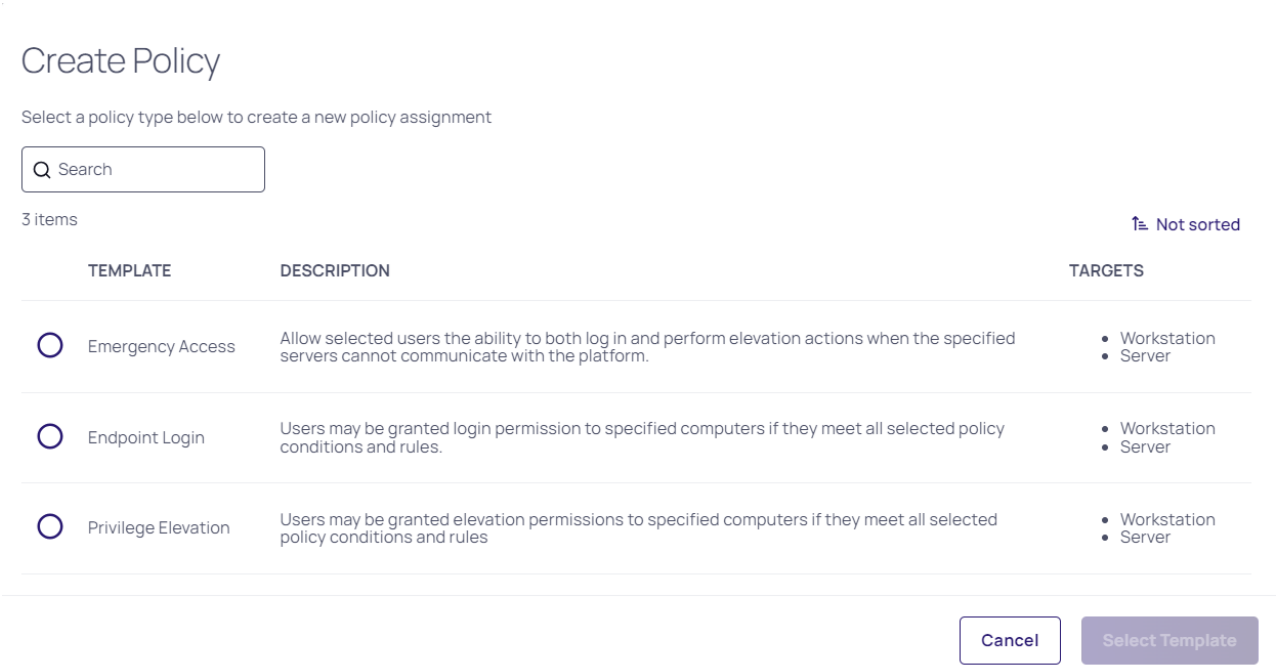
The deployment status refers to the deployment of the policy on the target, and can be Active, Activating, Activation Failed, Deactivating, Deactivation Failed, or Inactive. The Activating and Deactivating statuses appear for just a few seconds.



Create a Policy

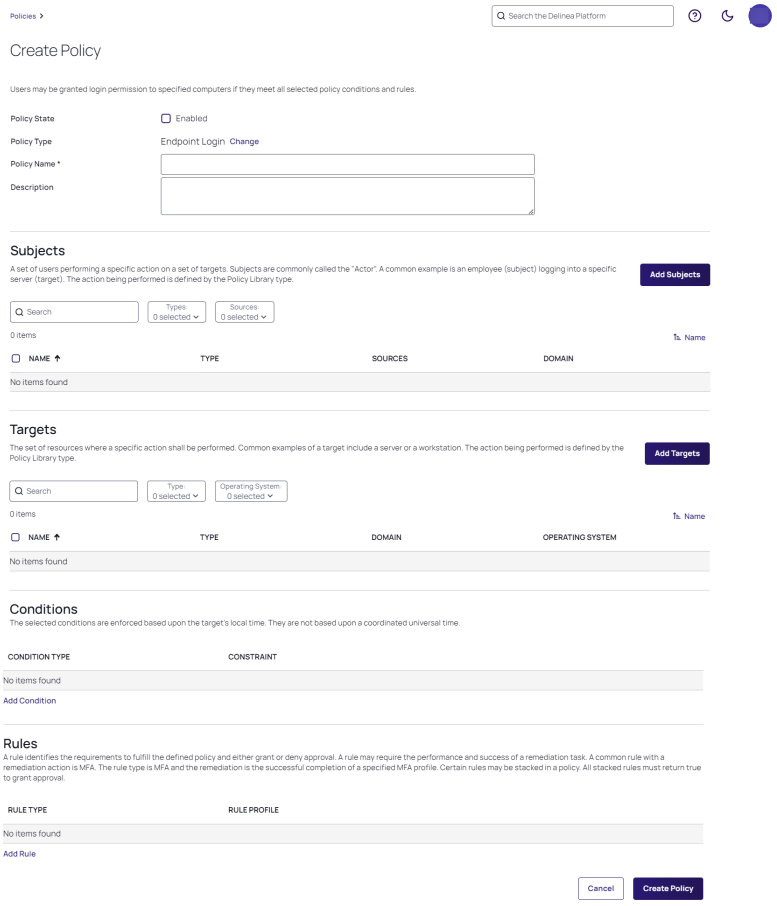
1. Click **Policies** from the left navigation menu. The Policies page opens, listing each policy available in your platform environment.
2. Click **Create Policy**.

3. On the Create Policy page, click a radio button to select a policy template from among the types listed, then click **Select Template**. A policy template is defined by the events you want to control.



4. Create at least one policy using each of the three policy templates below, and create them in the order presented below:
   a. **Emergency Access.** When a computer managed by the Delinea Platform cannot communicate with the platform, platform-dependent requirements cannot be met, such as MFA. Emergency Access policies enable the user to log in to the computer and perform elevated actions on that computer in that disconnected state.
   b. **Endpoint Login.** An Endpoint Login policy enables the user to log in with standard user permissions to a computer managed by the platform. MFA and other rule types can be enforced at login within this policy.
   c. **Privilege Elevation.** Privilege Elevation policies enable the user to temporarily elevate their own privileges for individual operations on the specified computer. Each elevated privilege action is controlled, tracked, and audited. MFA and other rule types can be enforced at elevation request within this policy.

      The user must be present in a separate Endpoint Login policy for privilege elevation to be granted.
5. After you click **Select Template**, a page opens where you can create a new policy, with the name of the base template (or policy type) displayed at the top.



Policy Details

1. At the top of the page, select the box next to Enabled to enable the policy.
2. Enter a policy name in the **Name** field.
3. Enter a policy description in the **Description** field.

Policy Subjects

1. Scroll down to the **Subjects** section to see a list of available subjects. Subjects are the users and user groups your policy can apply to, based on the template you selected earlier.
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

1. Scroll down to the **Targets** section. Targets are the computers and computer groups your policy can apply to, based on the template you selected earlier.
2. Click the **Add Targets** button.
3. Select the box next to each computer and computer group your policy will apply to.
4. Click the **Update** button.

Note: To be shown as a Target in a policy, a computer or computer group must have an agent installed.

Policy Conditions

1. Scroll down to the **Conditions** section. Conditions define when or how the policy should by applied. Conditions are optional. If a policy has a time range condition, the policy will apply only within that time range. If a policy has no time range condition, the policy will apply at all times.
2. Click **Add Condition**.
3. Click inside the *Search or pick one* box below **Condition Type.**
4. Select one of the condition types displayed or enter text to search. When you have selected a condition type, options will 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 Rules

1. Scroll down to the **Rules** section.
2. Click **Add Rule**. A policy rule can be set two ways:
   - **Allow**: Select **Allow** to permit access without requiring MFA. The user can log in without passing MFA challenges, so no Rule Profile (or Identity Profile) is needed. Emergency Access profiles always have the Allow rule applied, so no Rule Profile options are presented.
   - **MFA**. Select **MFA** to require multi-factor authentication. If you select MFA, a new *Search or pick one* box appears below **Rule Profile**. A Rule Profile must be used to specify which MFA challenges the user must pass, as well as the time allowed to elapse before the user is re-prompted for authentication. Select an authentication profile from the ones presented.
   - **Require Session Recording**: Select Require Session Recording to deny access if session recording cannot be performed on the endpoint, for example 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 rule, or in conjunction with either Allow or MFA. Require Session Recording can be also be applied to privilege elevation.
3. Scroll down to the **Rules** section.
4. Click **Add Rule**.

5. Select **MFA** to require multi-factor authentication or select **Allow** to permit access without requiring MFA.

> Emergency Access profiles always have the Allow rule applied, so no Rule Profile options are presented.

6. If you select MFA, a new *Search or pick one box* appears below **Rule Profile**.
7. Select an authentication profile from the ones presented.
8. When you have made all the required changes, click the **Create Policy** button in the bottom right corner.
9. Click **Activate** to activate the policy.

Setting up Audit and Session Recording

1. Click **Insights** from the left navigation menu.
2. Click **Session review** from the secondary menu.
3. Log into the server as the administrator, root, or normal AD user

Configure on Linux:

1. Log in as root user.
2. Enter commands:
   a. dacontrol -i DelineaPlatformAudit
   b. dacontrol -e
   c. dainfo

Configure on Windows:

1. Log in a Domain Administrator.
2. Launch **Agent Configuration**.
3. Click **Add Service**.
4. Select **Auditing and Monitoring Service**.
5. Click **OK**.
6. On Enable session capture and replay page, select **DelineaPlatformAudit**.
7. Click **Next**.
8. Audit and Monitoring configuration is complete.

Viewing Audit Session Recordings

On the platform, click **Insights**, then click **Session review**.

Log into the Linux and Windows servers as the administrator, root, or normal AD users

Linux

1. Run commands as root user.
2. Run commands as normal AD users.
   a. Elevate Commands as a normal AD users having the elevated permission policy using the dzdo command.

Windows

1. Run programs as the administrator.
2. Run commands as a normal AD user.
   a. Launch elevated desktop as a normal AD user having the elevated permission policy.

Setting up Use My Account for *nix Systems

Setup 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

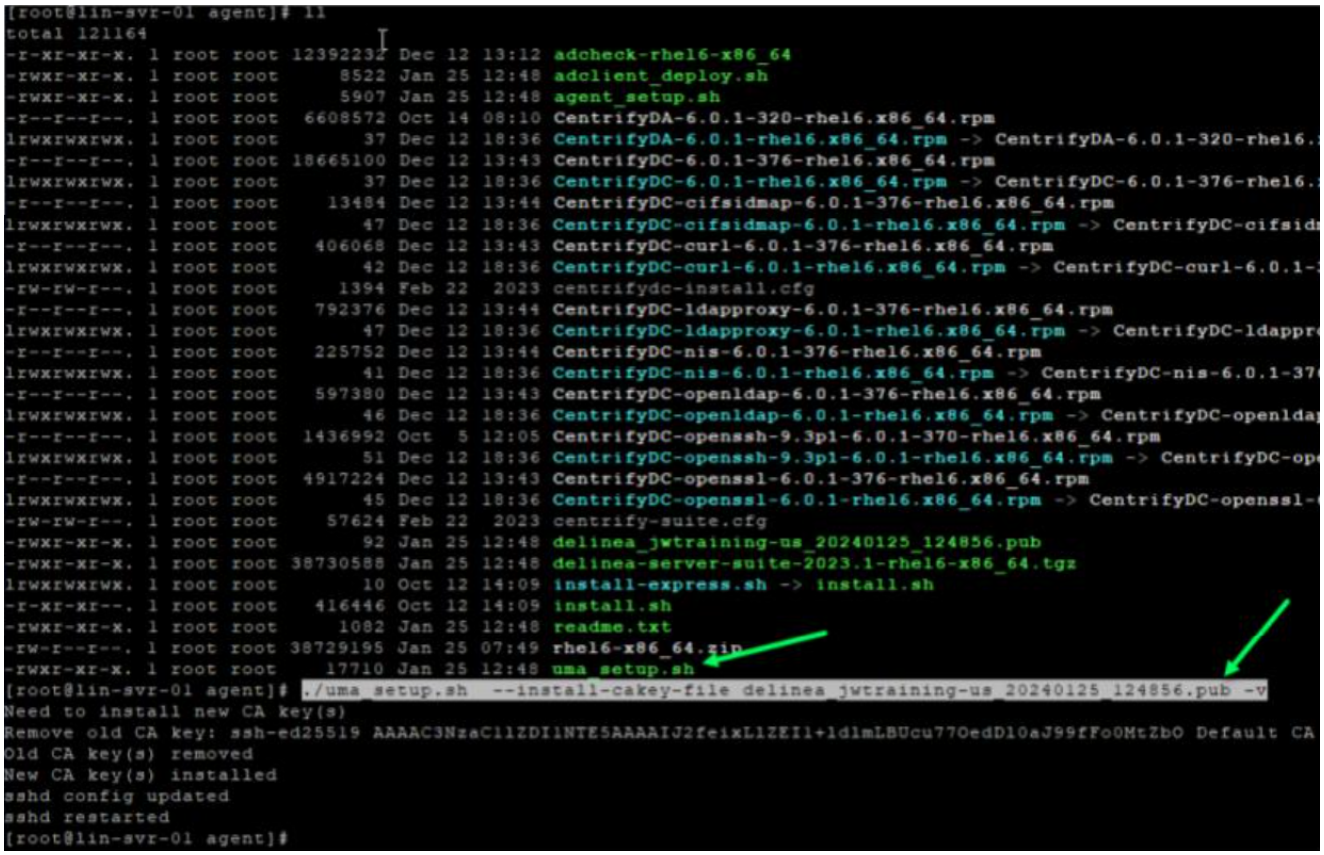
Note: The `agent_setup.sh` script automatically sets up UMA during the agent installation process.

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
```

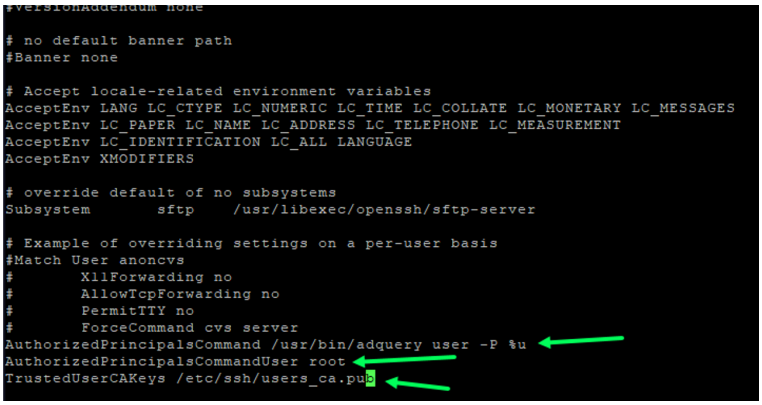
Example: `./uma_setup.sh --install-cakey-file delinea_jwtraining-us_20240125_124856.pub -v`



Manual Steps

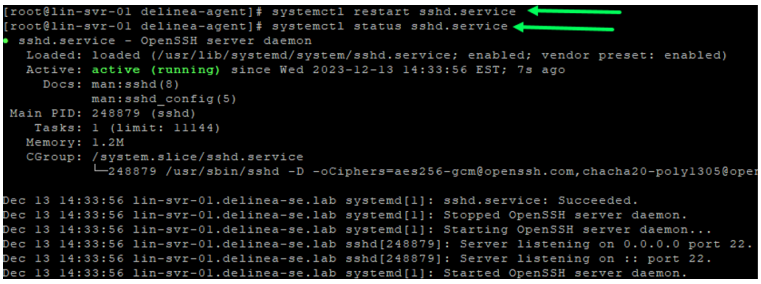
1. Navigate to and open the folder where you downloaded the agent from the Delinea Marketplace. The agent is a .pub file in the following format: `delinea_{tenant-name}_{download-date}.pub`
2. Copy the pub file to the ssh directory. Example:
   a. `cp delinea_{tenant-name}_{download-date}.pub /etc/ssh/users_ca.pub`
      i. `cp delinea_fishing_20231213_041058.pub /etc/ssh/users_ca.pub`
3. Edit the `sshd_config` file but make a backup copy in case you need to revert back: `cp /etc/ssh/sshd_config /etc/ssh/sshd_config_121323bk`
4. Edit the `sshd_config` file with the following lines:
   a. Example command: `vi /etc/ssh/sshd_config`
   b. `AuthorizedPrincipalsCommand /usr/bin/adquery user -P %u`
   c. `AuthorizedPrincipalsCommandUser root`

d. `TrustedUserCAKeys /etc/ssh/users_ca.pub`



5. Restart OpenSSH Service

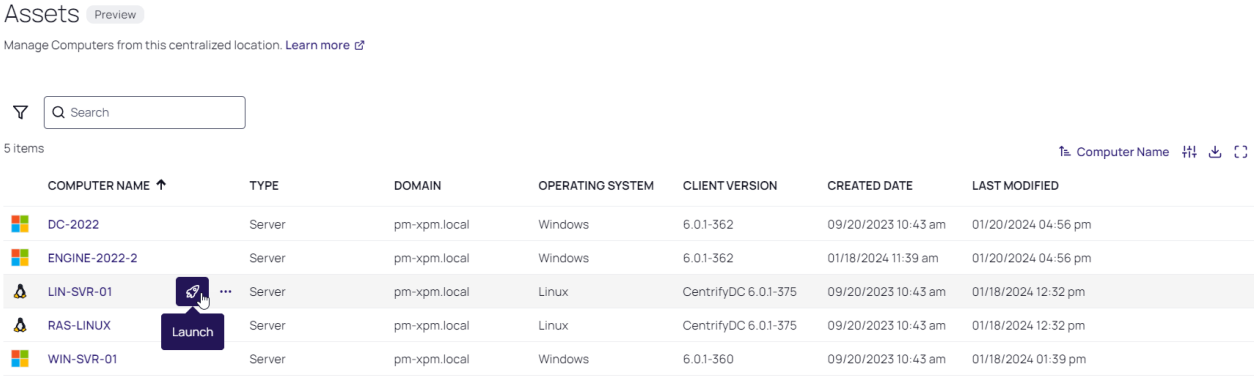
a. Example: `systemctl restart sshd.service`



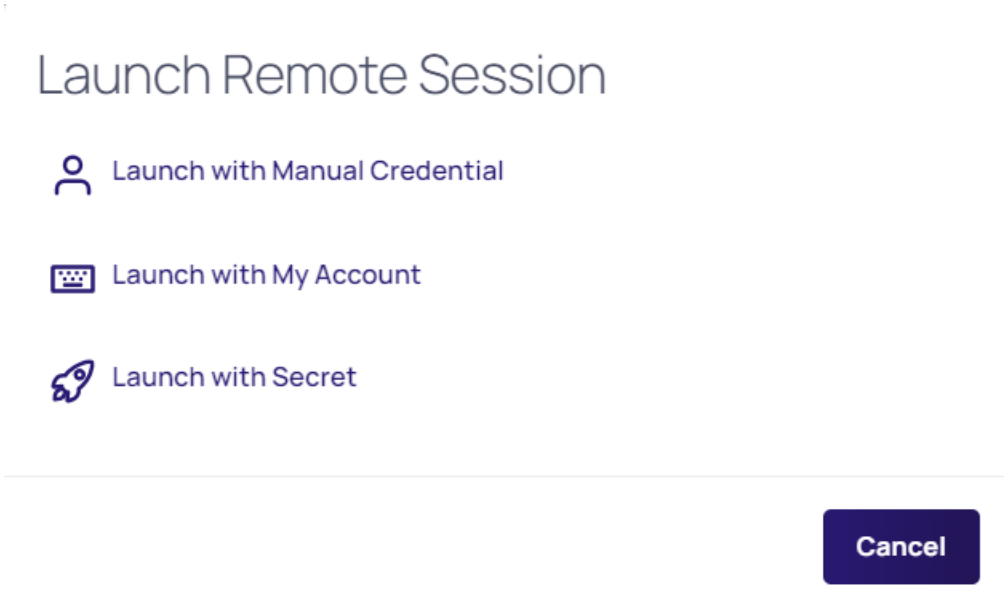
Testing Use My Account

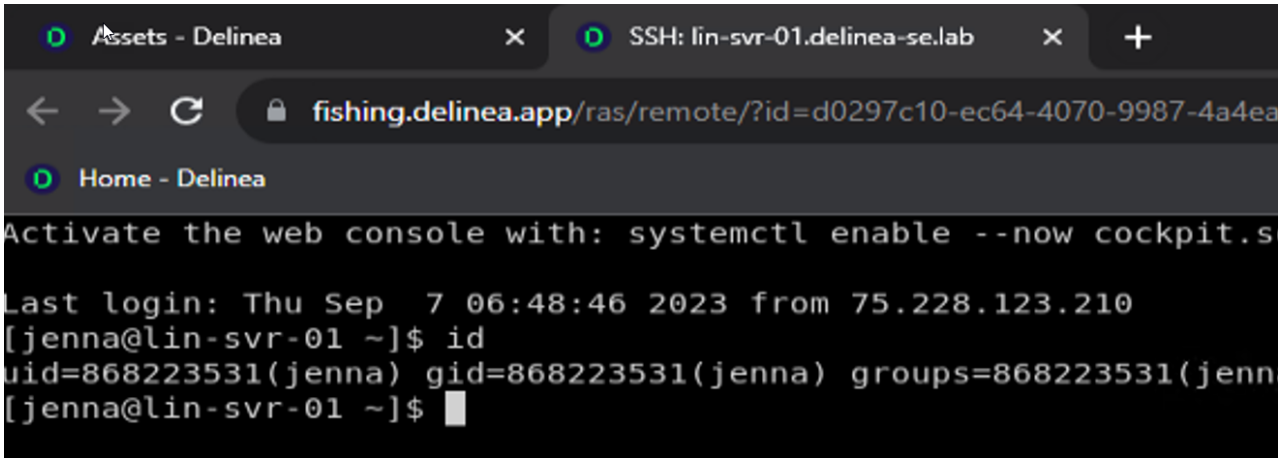
Note: UMA is only for *nix systems with the agent installed that is joined to the domain and zone.

1. Log in to the platform as an AD user with permission to log in to the Linux system.
2. Click **Inventory** from the left navigation menu.
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.



5. Select **Launch with My Account**.





Note: When reusing the same tenant for testing and the same SE Lab Template, make sure you delete all AD users from the platform.

Agents Reference

Installing Agents on Computers to be Managed

This section describes the recommended steps for deploying Privilege Control software on the nonWindows computers that you want to add to Active Directory. The chapter 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.

About the Deployment Process

There is no technical requirement that you only work with a subset of computers at a time, but in practice 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.

Select a Target Set of Computers

As a first step in preparing to install Privilege Control software, you should 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

You can:

- 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.

Install 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 on or switch to the root user if you are installing on a Linux or UNIX.
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.

Install 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 Available

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, you should 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, you can set the following parameters:

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_ldapproxy="K" Note that these additional packages may have dependencies or require a specific version of the Privilege Control Agent for *NIX to be installed. Before installing or updating additional packages silently, you should review the information in the Upgrade and Compatibility Guide. | 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:

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. Note that the install.sh script calls adcheck twice. After the first call, adcheck 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 adcheck 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 skipped. Set this parameter to Y if you want to run adcheck 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.
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 install.sh 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.

Parameter	Description
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.
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.

Parameter	Description
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.
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.

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_ldapproxy=”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

Use 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, etc, 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 agent package for platform-specific installation details.

About the Files and Directories Installed on the Agent

When you complete the installation, the local computer will be updated with the following directories and files for the core Privilege Control Agent for *NIX:

This directory	Contains
/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.

This directory	Contains
/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, that is, 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 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.

PCS Troubleshooting Guide

Issue: I don't know where to find all my log files.

Resolutions:

Delinea Connector

C:\Program Files\Delinea\Delinea Connector\log.txt

Delinea Engine

C:\ProgramData\Delinea Engine\<engine_version>\log

Command Relay

Command Relay stores logs in 2 places:

- **Abridged Log** - C:\ProgramData\Delinea Engine\<engine_version>\delinea\command-relay\<version>\log
- **Detailed Log** - C:\ProgramData\Delinea\CommandRelay\Logs

Privilege Control Agent

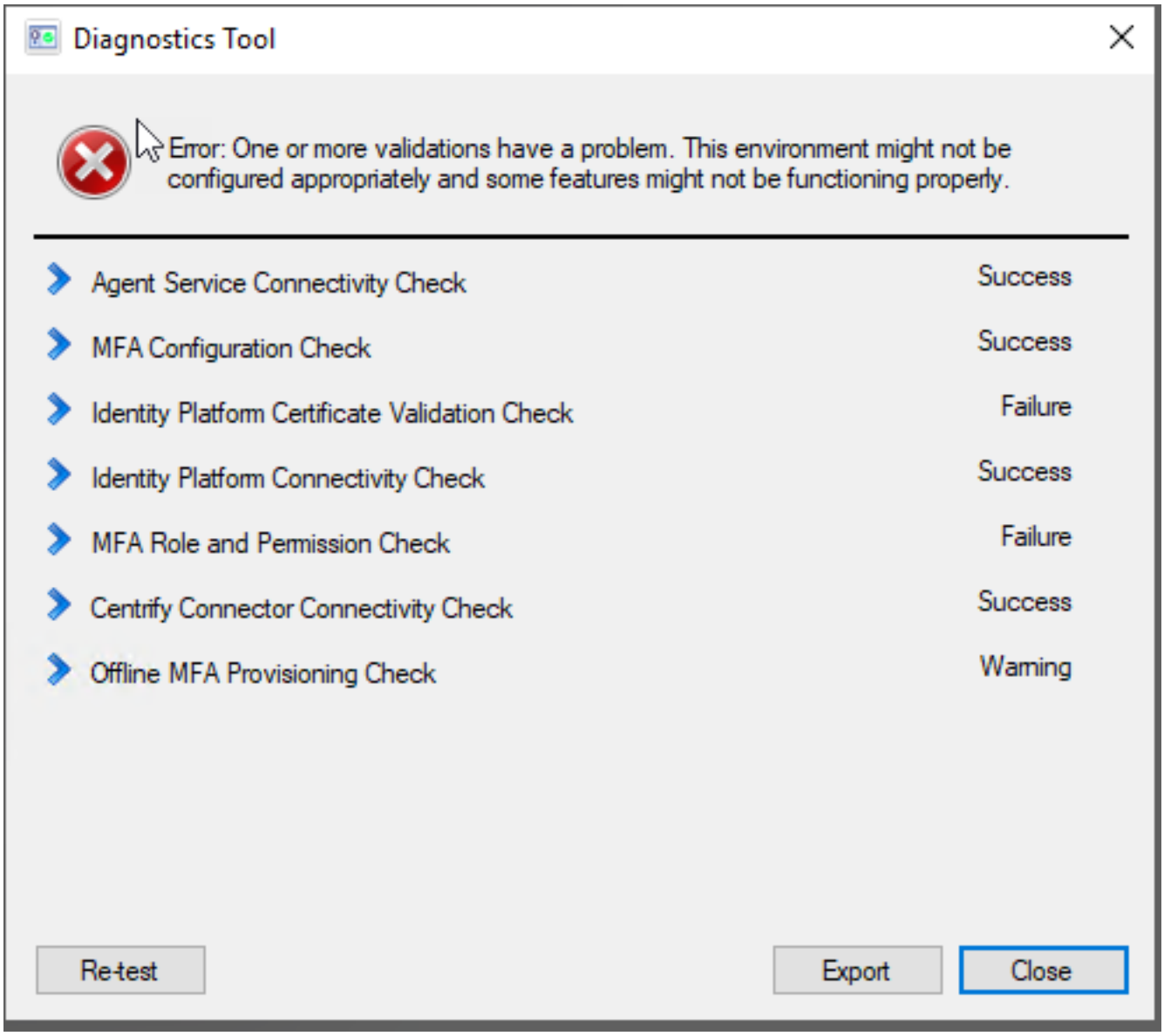
- **Linux** - /var/log/centrifydc.log
- **Windows** (default location): - C:\Program Files\Common Files\Centrify Shared\Logs\

You can change where the Windows agent log files are stored using Privilege Elevation Service Settings:

1. Open “Delinea Agent Configuration”
2. Click “Settings” button under “Privilege Elevation Service”
3. Go to “Troubleshooting” tab in “Privilege Elevation Service Settings” and click “Options” button
4. Change Log folder path as you want. You also could change the trace level in this “Options” dialog.

Issue: Windows Diagnostics Error for MFA

Error: One or more validations have a problem. The environment might not be configured appropriately and some features might not be functioning properly.



Resolution: This message indicates erroneously that MFA is not working for PCS. You can ignore this message.

Issue: How do I upgrade the Agent?

Resolution:

To upgrade the Agent on a host system, download the Agent package from the Delinea Marketplace. The installation script (`agent_setup.sh`) is included in the package.

`--upgrade` Upgrade selected packages on the system.

For example:

```
./agent_setup.sh --upgrade --install-openssh
```

Policies

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**.
3. If the message reads, "Connector is not available," select the Connector tab and click **Start**.
4. If the message reads, "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.
5. If your known user or all users are still not showing up in your search to a policy target, check the Connector logs and contact Delinea support if necessary.

Issue: My Policy is stuck on “Activating” (or “Deactivating”) status?

Resolution: Normally a Policy stuck on Status “Activating” or “Deactivating” is a indication of problem with the Command Relay. Please check if you have a Command Relay running. For more **Command Relay** debug options, please see Command Relay / Engine Pool section below.

Issue: My Policy status is “Active” but it's not being enforced.

Resolution: Policy changes may take up to 30 minutes to be enforced after its status becomes Active or Inactive, due to the agent internal caching. If Policy is not being enforced after that time, please notify Delinea support.

Issue: My Login (or Elevation) Policy status is “Inactive” but I can still perform Login (or Elevation) on the machine. Why?

Resolution: Policy changes may take up to 30 minutes to be enforced after its status becomes Active or Inactive, due to the agent internal caching. If Policy is not being enforced after that time, please notify Delinea support.

Issue: The Policy’s Target list is not showing the machine I want to select.

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, please check if that same machine appears in the Inventory list.

If the machine not listed under Targets is listed under **Inventory**, please notify Delinea support.

If the machine not listed under Targets is **also not** listed under **Inventory**, then you need to “Discover” that machine by doing a Secret Server Discovery process.

Command Relay / Delinea Engine

Command Relay is one of the workloads deployed by the Delinea Engine and heavily depends on the Engine to run. Therefore, when troubleshooting Command Relay it is also important to investigate potential problems with the

Engine. Currently the main tool for Command Relay troubleshooting is looking at the logs that are saved by Command Relay.

Issue: How do I turn on debugging for my Engine?

Resolution: The default setting for **Engine Pool** logs ensures the logging of critical errors only without much detail. If you want detailed information, increase the default 'verbose' level to "Debug" in the Engine Pool's `appsettings.json` file (Logging Level)

`C:\Program Files\Delinea Engine\<engine_version>\appsettings.json`

Issue: Is Delinea Command Relay setting in Engine Pool for all engines under the same site?

Resolution: Yes. You could create another site if you want to user a different domain.

Issue: Why does Command Relay need the Active Directory domain admin credentials?

Resolution: Command Relay uses the credentials to communicate with AD to store the Policies. By default, AD users in "Domain Admins" group have all the required permissions.

Issue: What happens if I provide the wrong Active Directory domain admin credentials or if they expire?

Resolution: Command Relay will stop working (and therefore no other Policy change would be applied) and you would see in the Command Relay log the following:

```
2024-02-01 06:59:22,052 [6] ERROR CommandRelay [(null)] - Failed to run workload
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.
 ---> Delinea.CommandRelay.Common.LogonException: Invalid Domain Credentials. Logon user
failed: Administrator, errorCode=1326
 ---> System.ComponentModel.Win32Exception (1326): The user name or password is incorrect.
   --- End of inner exception stack trace ---
   at Delinea.CommandRelay.Common.RunAsProcess.Run(String cmd, String workDir) in
   D:\a\1\s\Delinea.CommandRelay.Common\RunAsProcess.cs:line 195
   at Delinea.CommandRelay.Setup.RunLocalProcess(String cmd) in
   D:\a\1\s\CommandRelay\Setup.cs:line 287
   at Delinea.CommandRelay.Setup.ValidateEnv() in D:\a\1\s\CommandRelay\Setup.cs:line 210
   at Delinea.CommandRelay.DomainCredsHandler.ValidateCreds(CancellationToken stoppingToken)
   in D:\a\1\s\CommandRelay\DomainCreds.cs:line 64
   --- End of inner exception stack trace ---
   at Delinea.CommandRelay.DomainCredsHandler.ValidateCreds(CancellationToken stoppingToken)
   in D:\a\1\s\CommandRelay\DomainCreds.cs:line 82
   at CommandRelay.TaskService.Initialize(HostClient client, CancellationToken
   stoppingToken) in D:\a\1\s\CommandRelay\TaskService.cs:line 235
   at CommandRelay.TaskService.Run(HostClient client, CancellationToken stoppingToken) in
   D:\a\1\s\CommandRelay\TaskService.cs:line 54
   at Delinea.CommandRelay.WorkloadWorker.ExecuteAsync(CancellationToken stoppingToken) in
   D:\a\1\s\CommandRelay\Workload.cs:line 66
Failed to run deployment: Command execution failed because the underlying process (
CommandRelay.exe#2160) returned a non-zero exit code (3).
```

Issue: My selected secret for Command Relay stopped working (domain admin account)

Resolution: This could happen if the selected secret is changed, e.g. if you moved the secret to a personal folder in Secret Server, it will remove the EngineWorkload shared permissions on the secret which will cause permission failure in Command Relay.

Resolution: This could also happen if the underlying domain account associated with this secret is changed, e.g. password expired/not synced, account locked, AD permissions removed, etc. There will be a log on failure log with error details about those.

Issue: Command Relay can't log in using the same secret that works for Secret Server Discovery service?

Resolution:

In the Command Relay log, you see that the Command Relay cannot login:

2024-01-29 14:17:11,592 [10] INFO CommandRelay [(null)] - RunAsProcess info: domain=eric-sp-1.eric user=svc-ssd

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.

Secret Server

Issue: My Secret Server Distributed Engine is not working.

Resolution: Check if the Engine has been Activated

Resolution: Check if the Windows clock of the machine where the agent is running is correct

Privilege Control for Servers Agent

Issue: How do I turn on/off debugging for Linux agents?

Resolution: To turn on debugging, run the following commands as the root user:

- `/usr/share/centrifydc/bin/addebug set cloud.object TRACE`
- `/usr/share/centrifydc/bin/addebug on`

Logs can be found in `/var/log/centrifydc.log`.

To turn off debugging, run the following commands as the root user:

`/usr/share/centrifydc/bin/addebug off`

Issue: How do I turn on debugging for the sshd server?

Resolution:

Run `ps -ef | grep sshd` to check if you are using CentrifyDC-openssh or system stock sshd.

If you are using CentrifyDC-openssh

1. add `LogLevel DEBUG3` into `/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` into `/etc/ssh/sshd_config`
2. restart the server by running this command as the root user: `systemctl restart sshd` (or `systemctl restart ssh` on Ubuntu/Debian)

Issue: How do I collect debug info for the Delinea team to investigate an issue?

Resolution:

1. Turn on debugging for Linux agent and sshd
2. Reproduce the issue
3. Run `adinfo -t` command as the root user

the /var/centrify/tmp/adinfo_support.tar.gz file is what the Delinea support team will need for investigation.

Issue: My AD forest has multiple domains, so will each domain have a DelineaZone created?

Resolution:

No, there will be only one DelineaZone created in the forest when you deploy the very first Engine Pool in the forest.

Issue: My AD user cannot log in to the domain-joined Linux machine

Resolution:

You will need a root shell for the following steps.

Suppose your AD user name is “tom@acme.com”

1. Please note it may take up to 30 minutes before the Linux agent refreshes the latest authentication and authorization info from AD after the policy deployment. You can also manually run adflush -f to force a refresh at any time.
2. Verify whether the AD user is visible on the Linux machine
   - adquery user tom@acme.com
     - If you get “tom@acme.com is not a zone user”, please verify whether the Command Relay has successfully deployed the policy.
3. Verify whether the AD user has login permissions

- dzinfo --role tom@acme.com
  - an example output would look like this:

```
User: tom
Forced into restricted environment: No
MFA Service authentication: Supported
Privileged commands:
Name             Avail Command               Source Roles
---------------  ----- --------------------  --------------------
__pe_sys_6240d3  No    *                     Mansion-Grove-Elevat
33-6256-4221-9a                              ion/DelineaZone
23-39bfc381202c
/DelineaZone
__pe_6240d333-6  No    *                     Mansion-Grove-Elevat
256-4221-9a23-3                              ion/DelineaZone
9bfc381202c/Del
ineaZone
...
...
```

If you don't see "Password login" and "Non password login" in the "Effective rights", please verify whether the Command Relay has successfully deployed the policy.

If both adquery and dzinfo commands show the expected result, please collect debug info and contact Delinea support.

Issue: My AD user can't run DZDO commands in the domain-joined Linux machine

Resolution:

You will need a root shell for the following steps.

Suppose your AD user name is "tom@acme.com"

1. Please note it may take up to 30 minutes before the Linux agent refreshes the latest authentication and authorization info from AD after the policy deployment. You can also manually run adflush -f to force a refresh at any time.
2. Verify whether the AD user has privileged command rights
   - dzinfo --commands tom@acme.com
     - an example output would look like this

```
User: tom
Forced into restricted environment: No
MFA Service authentication: Supported
Privileged commands:
Name             Avail Command               Source Roles
```

```
---------------  ----- --------------------  --------------------
__pe_sys_6240d3  No    *                     Mansion-Grove-Elevat
33-6256-4221-9a                              ion/DelineaZone
23-39bfc381202c
/DelineaZone
__pe_6240d333-6  No    *                     Mansion-Grove-Elevat
256-4221-9a23-3                              ion/DelineaZone
9bfc381202c/Del
ineaZone
...
...
```

If you don't see anything in the "Privileged commands", please verify whether the Command Relay has successfully deployed the policy.

If dzinfo command shows the expected result, please collect debug info and contact Delinea support.

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.

Issue: I need Some Useful Commands and Tips for AD Client on *.nix

Resolution:

AD-bridging commands ("ad" commands)

adinfo - provides information about the status of the agent

Looking-up Basic Information

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 the status (mode) of the agent (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

$ adinfo --zonedn (in distinguishedName format)

Advanced/Troubleshooting Information

DNS

To check for the "joined-as" name (local host name and joined as name may 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 against 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

To perform Auto-enrollment of Computer PKI Certificates (requires elegible template and communications)

Using the computer object to authenticate: $ dzdo /usr/share/centrifydc/sbin/adcert --enroll --machine

Using a user to authenticate: $ dzo /usr/share/centrifydc/sbin/adcert --enroll --user [ADusername]

Testing a user's password: $ adinfo -A --user [username] #
This will prompt you for a password, the output is: Password for user "username" is correct/incorrect

Dynamic DNS

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 (e.g. eth0): $ sudo addns --update --machine --interface eth0

Querying Delinea-enabled AD Users and Groups:

adquery - provides information about Active Directory users and groups that are UNIX-enabled by Delinea

To view all Delinea UNIX-enabled users: $ adquery user will show all AD users in Express mode / Only authorized in Zone mode

To view all Delinea UNIX-enabled groups: $ adquery group will show all AD groups in Express mode / Only unix-enabled in Zone mode

To view a user's entry (UNIX passwd file style): $ adquery user [username]

To view a group entry (UNIX group filestyle): $ 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 distinguishedName 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

adflush - clears the Delinea cache in the local computer (dc, gc, credential & 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 carefully): $ 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 (in MFA scenarios): $ dzdo adflush --connectors

Group Policy-related Commands

adgpupdate - 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

adgpresult - to view a RSOP (resultant set of policy) to 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: $ adgpresult --user

To view the report for a particular user: $ dzdo adgpresult --user [user.name]

Joining Active Directory

adjoin - joins an Active Directory domain

To run adjoin successfully, you need the following:

- to be root or sudo
- to have the credentials (or the keytab) of an AD user that can join computers to a container (NOT Domain Admin)
- to know the Distinguished Name (e.g. "ou=servers,ou=unix") of the container that you will place the system in AD
- to know the domain name you're joining
- to have a clear network path to the DC or DCs you're using (dns, global catalog, kerberos, ldap, cifs, ntp).

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 (AD/Delinea admin pre-created the machine ahead of time using Access Manager or Delinea Poweshell cmdlets): $ sudo adjoin --selfserve [domain.name]

To join AD in zone mode (e.g. 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 (must know what you're doing - 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: $ suod adjoin --licensetype "workstation"--workstation --container "ou=workstations,ou=unix" --user [AuthorizedADUser] --verbose [domain.name]

To use an specific domain controller to join (e.g. 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 algorighm 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 (e.g. adserver vs. 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]

Leaving Active Directory

adleave - leaves an Active Directory domain

To run adleave successfully, you need:

- > sudo or root
- > for online leave, authorized AD user credentials

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

Privilege Elevation ("dz" commands):

dzinfo - displays information of 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 elevation): $ dzinfo --computer-role

To view authorization information about about another user (requires elevation): $ dzdo dzinfo [user.name]

To test a command against the role: $ dzinfo --test [path/to/binary] [options]

Delinea -enhanced sudo

dzdo - delinea-enhanced sudo. Uses Delinea zone data in AD for commands, otherwise identical to sudo.

To view version information (as of 2015, based on sudo 1.8.10p3): $ dzdo -V

DirectAudit Commands ("da" commands)

dainfo - 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 (must elevate): $ dzdo dainfo --username lisa.simpson

dacontrol - controls the status/configuration of the directaudit client (requires 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

What Happens When adjoin is Run Succesfully?

This activates the DirectControl agent (adclient/ DelineaDC service):

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, session modules. A back-up of the previous configuration is made.
7. The NSS (Name Service Switch) providers for users and groups defaults to AD first, then other methods (e.g. files, ldap, etc). A backup of the previous configuration is made. Note: in the OS X platform, the PAM/NSS functions are channeled via 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/rights defined.
10. User/Group identity (RFC2307) data in AD is stored within the Delinea zone, NOT with the user/group object.
11. The virtual registry is initialized and group policies are enforced.

What Happens When adleave is Run Successfully?

1. Online the --remove object: The object in AD is removed from the container and from the zone (frees license)
2. Online the without --remove object: The object in AD is marked as disabled. Must be ovewritten to rejoin.
2. Offline: The object in AD is left orphaned. Cleanup must happen via any Delinea API (AM, PowerShell, adedit)
3. The UNIX environment is reset and rolled back (Kerberos, PAM, NSS)
4. The Delinea adclient (DelineaDC) service is disabled.

Important Files and Folders

/usr/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

Note: on OS X El Capitan, things changed to /usr/local/share/centrifydc

/etc/centrifydc

centrifydc > config files for the DirectControl agent

centrifyda > config files for the DirectAudit agent

centrifycc > config files for the Privilege Service CLI Toolkit for AAPM

openldap > config files for Delinea-enhanced OpenLDAP proxy if installed

ssh > config files for Delinea-enhanced OpenSSHls

/var/centrifydc

kset* files > dynamic information about the environment

reg > virtual registry, contains the computer and user hives (user GPO disabled on Servers)

/var/centrify

net/certs > location of any Microsoft Certificate Authority auto-enrolled certs, keys and trust chain

Issue using DirectControl Authentication on *NIX systems

When the directory /var is NFS mounted, DirectControl may not work properly.

Resolution

Directory /var should not be NFS mounted or else DirectControl may not work properly.

PCS Technical Reference

Storing Privilege Control Properties in Active Directory

The Active Directory schema defines the object classes that can be stored in Active Directory, and the attributes that each object class must have, plus any additional attributes the object can have, and the object class that can be its parent. Schema definitions are also stored as objects in Active Directory. To store UNIX-specific attributes within the Active Directory schema, the schema must be able to include the properties that are associated with a UNIX user or group. For example, for a UNIX user, the schema needs to accommodate the following information fields:

- UNIX user name
- Password hash (optional)
- Numeric user identifier (UID)
- Primary group identifier (GID)
- General information (GECOS)
- Home directory
- Default shell

Some of these information fields are similar to standard user class attributes in Active Directory. For example, the Active Directory Display Name (displayName) attribute typically stores a user's full name—the same information typically stored in the GECOS field in an /etc/passwd file on a UNIX computer, so the displayName is used to define the contents of the GECOS field in a user's UNIX profile. Depending on the Active Directory schema you have

installed, some of the information fields required for logging on to UNIX computers might not have an equivalent Active Directory attribute.

If you are using the default Active Directory schema, Privilege Control stores UNIX-specific attributes in an Active Directory class under its own parent container for zones. Privilege Control then organizes the information about individual UNIX computers, users, and groups by zone.

Core Agent Components and Services

The Privilege Control Agent makes a UNIX or Linux computer look and behave like a Windows computer to Active Directory. Once installed, the agent performs the following key tasks:

- Joins UNIX or Linux computers to an Active Directory domain.
- Communicates with Active Directory to authenticate users logging on to the UNIX or Linux computer, and caches credentials for offline access.
- Enforces Active Directory authentication and password policies.
- Extends Active Directory group policies to manage the configuration of UNIX users and computers.
- Provides a Kerberos environment so that existing Kerberos applications work transparently with Active Directory.

Individual agents are platform-specific, but provide an integrated set of services to extend Active Directory authentication, authorization, and directory service to managed computers. The following figure provides a closer look at the services provided through the Privilege Control Agent:

As this figure suggests, the agent typically includes the following core components:

- The core component of the agent is the adclient process that handles all of the direct communication with Active Directory. The agent contacts Active Directory when there are requests for authentication, authorization, directory assistance, or policy updates, and then passes valid credentials or other requested information along to the programs or applications that need this information.
- The core component of the agent is the adclient process that handles all of the direct communication with Active Directory. The agent contacts Active Directory when there are requests for authentication, authorization, directory assistance, or policy updates, and then passes valid credentials or other requested information along to the programs or applications that need this information.
- The **Delinea Pluggable Authentication Module**, pam_centrifydc, enables any PAM-enabled program, such as ftpd, telnetd, login, and sshd, to authenticate using Active Directory.

  Note: For AIX, the implementation is slightly different. For example, the agent for AIX can use PAM interfaces if you have configured the computer to use PAM modules or the interfaces in the Loadable Authentication Module (LAM) to handle behavior that on other platforms is done through PAM or NSS.

- The **Delinea NSS module** is added to nsswitch.conf so that system look-up requests use the agent to look up and validate information using Active Directory through LDAP.
- The **Privilege Control-managed Kerberos environment** generates a Kerberos configuration file (etc/krb5.conf) and a default key table (krb5.keytab) file to enable your Kerberos-enabled applications to authenticate through Active Directory. These files are maintained by the agent and are updated to reflect any changes in the Active

Directory forest configuration.

- The **Privilege Control local cache** stores user credentials and other information for offline access and network efficiency.

In addition to these core components, the agent can also be extended with the additional software packages, including modified versions of programs such as Kerberos command line tools, OpenSSH and OpenLDAP utilities. Privilege Control-enabled versions of these programs allow you to use Active Directory accounts and Kerberos credentials for authentication, authorization, and policy enforcement services.

Key Operations Handled by the Adclient Process

The most important element in the agent is the adclient process. The adclient process runs as a single trusted service. This process is automatically added as a boot service and is started whenever you reboot a managed computer. The adclient process handles all of the direct communication with Active Directory and manages all of the operations provided through the other services.

The adclient process performs the following key tasks on managed computers:

- Locates the appropriate domain controllers for the local computer based on the Active Directory forest and site topology published by the Windows DNS server. If a domain controller becomes unavailable, the adclient process automatically locates the next available domain controller to ensure uninterrupted service.
- Provides Active Directory with credentials for the local computer account to verify the computer is a valid member of the domain.
- Delivers and stores user credentials so that users can be authenticated by Active Directory and, once authenticated successfully, can sign on even if the computer is disconnected from the network for mobile access or if Active Directory is unavailable.
- Caches query responses and other information, including positive and negative search results, to reduce network traffic and the number of connections to Active Directory and to ensure users can work uninterrupted and start new application sessions using their existing login credentials. All communication with Active Directory is encrypted to ensure security, and you can manage the cache through configuration parameters or group policy.
- Creates and maintains the Kerberos configuration and service ticket files to allow existing Kerberos-enabled applications to work with Active Directory without any manual configuration.
- Synchronizes the local computer's time with the clock maintained by Active Directory to ensure the timestamp on Kerberos tickets issued by the KDC are within a valid range.
- Resets the password for the local computer account in Active Directory at a regular interval to maintain security for the account's credentials.
- Provides all the authentication, authorization, and directory look-up services retrieved from Active Directory to the other Privilege Control Agent services, such as the PAM service authentication module.

How PAM Applications Work with Privilege Control

Pluggable Authentication Modules (PAM) are a common mechanism for configuring authentication and authorization used by many UNIX programs and applications. If a program or application uses PAM for authentication and authorization, the rules for authenticating the user are configured in either the PAM configuration file, /etc/pam.conf or in application-specific files in the /etc/pam.d directory.

The Privilege Control Agent for *NIX includes its own Pluggable Authentication Module (pam_centrifydc) that enables any application that uses PAM, such as ftpd, telnetd, login, and Apache, to authenticate users through Active Directory. When you join a domain, the pam_centrifydc module is automatically placed first in the PAM stack in systemauth, so that it takes precedence over other authentication modules.

The pam_centrifydc module is configured to work with adclient to provide a number of services, such as checking for password expiration, filtering for users and groups, and creating the local home directory and default user profile files for new users. The services provided through the pam_centrifydc module can be customized locally on a computer, modified through Active Directory group policy, or configured through a combination of local and Active Directory settings.

Working in conjunction with the adclient process, the pam_centrifydc module provides the following services for PAM-enabled programs and applications:

- Requests the PAM-enabled application to prompt for a password when appropriate and verifies whether the application-provided user name and password are valid in Active Directory.
- Checks whether the user's password has expired in Active Directory. If the password has expired, the pam_centrifydc module prompts the user to change the password, and forwards the new password to the adclient process, which communicates the change to Active Directory.
- Queries the adclient process to determine whether any access control policies are applied. For example, the pam_centrifydc module uses the information in the centrifydc.conf file to determine whether a local user attempting to log on is mapped to an Active Directory account, whether specific users or groups have been granted or denied permission to log on to the local computer, or whether Active Directory authentication should be ignored for a specific user or group.
- Creates the local home directory and default user profile files for new users. The pam_centrifydc module uses skeleton files to set up the user environment when new Active Directory users log on to a managed computer for the first time.

Most of these tasks are performed during a user login session as a series of requests and replies from the pam_centrifydc module to Active Directory through the adclient process for those programs and applications that are configured to use PAM. Because PAM is the most common authentication service used by UNIX programs and applications, the pam_centrifydc module is the most commonly used for a typical log-on session. For a more detailed description of a typical log-on process, see What happens during the typical log-on process.

Note: The order in which identity stores are listed in the nsswitch.conf file does not influence authentication. Authentication and authorization services are provided by Active Directory through the Privilege Control Agent for *NIX and its PAM component, and by default, Active Directory is always tried before any other sources. The order in which sources are checked is controlled through the PAM configuration settings, for example, the lines defined in the pam.conf file. In general, you should not modify the PAM configuration because making changes to these settings can compromise security or produce unexpected and undesirable results.

How NSS Configuration Works with Privilege Control

The Name Service Switch (NSS) provides a mechanism for identifying sources of network information a computer should use, such as local password and group files, NIS maps, NIS+ tables, LDAP, and DNS, and the order in which these sources should be consulted when looking up users, groups, host names, and other information.

When you join a domain, the NSS configuration file, nsswitch.conf, is automatically updated to use the Privilege Control Agent's NSS module first. Using the adclient process and the service library, the Privilege Control NSS module accesses network information that's stored in Active Directory through LDAP.

When a UNIX program or application needs to look up information, it checks the nsswitch.conf file and is directed to use the nss_centrifydc module. The nss_centrifydc module directs the request to Active Directory through the adclient process. The adclient process provides the information retrieved from Active Directory, then caches the information locally to ensure faster performance, reduce network traffic, and allow for disconnected operation.

Note: The order in which identity stores are listed in the nsswitch.conf file does not influence authentication. Authentication and authorization services are provided by Active Directory through the Privilege Control Agent and its PAM service, so Active Directory is always tried before any other sources, regardless of what you have specified in the nsswitch.conf file. Instead, the nsswitch.conf file determines the sources to use in responding to NSS queries such as getpwnam. In general, you should not modify this file because modifying the file can compromise security and complicate auditing activity. In addition, you should not specify ldap as a source in any nsswitch.conf file where you have installed the Privilege Control Agent. Specifying ldap in the nsswitch.conf file can cause the system to crash.

How the Privilege Control Agent Manages Kerberos Files

Kerberos is a network authentication protocol for client/server applications that uses encrypted tickets passed through a central Key Distribution Center to verify the identity of a user or service requesting access. Because Kerberos is an industry standard and a secure network authentication mechanism, you may already have UNIX programs and services that are configured to use it. To allow those existing Kerberized applications to work with Active Directory without manual configuration, the adclient process automatically creates and maintains the Kerberos configuration file, krb5.conf, and the krb5.keytab service ticket file to point Kerberos-enabled services and applications to the Key Distribution Center (KDC) in Active Directory when you join a domain.

The configuration file is initially created using information collected by probing DNS and Active Directory with the default domain set to the domain that the computer has joined. Whenever a logon or ticket validation is performed with a domain that is not in the configuration file, the configuration file is updated so that it includes the new domain. Although the adclient process can automatically update the file as needed, it does not destroy existing configuration entries that you may have added by hand. Because of this, Privilege Control Agents work seamlessly with existing Kerberos-enabled applications.

Note: The Authentication Service supports users defined in a Kerberos realm as long as the Kerberos domains or realms are resolvable by DNS. Kerberos realm names are case sensitive, so be careful to check that the realm spelling and capitalization is correct.

What Happens During the Typical Log-on Process

The core Privilege Control Agent for *NIX components work together to identify and authenticate the user any time a user logs on to a computer using any UNIX command that requires the user to enter credentials. The following steps summarize the interaction to help you understand the process for a typical log on request. The process is similar, though not identical, for UNIX commands that need to get information about the current user or group.

Note: The following steps focus on the operation of the agent rather than the interaction between the agent and Active Directory. In addition, these steps are intended to provide a general understanding of the operations performed through the agent and do not provide a detailed analysis of a typical log on session.

When a user starts the UNIX computer, the following takes place:

1. A login process starts and prompts the user to supply a user name.
2. The user responds by entering a valid local or Active Directory user name.
3. The login process, which is a PAM-enabled program, then reads the PAM configuration file, /etc/pam.conf, and determines that it should use the Privilege Control PAM service, pam_centrifydc, for identification.
4. The login process passes the login request and the user name to the Privilege Control PAM service for processing.
5. The pam_centrifydc service checks the pam.allow.override parameter in the agent configuration file to see if the user name entered is an account that should be authenticated locally.
   - If the user should be authenticated locally, the pam_centrifydc service passes the login request to the next PAM module specified in the PAM configuration file, for example, to the local configuration file /etc/passwd.
   - If the user is not listed as an override account, the pam_centrifydc service continues with the login request and checks to see if the adclient process is running, then passes the login request and user name to adclient.
6. The adclient process connects to Active Directory and queries the Active Directory domain controller to determine whether the user name included in the request is a user who has access to computers in the current computer's zone.
   - If the adclient process is unable to connect to Active Directory, it queries the local cache to determine whether the user name has been successfully authenticated before.
   - If the user account does not have access to computers in the current zone or can't be found in Active Directory or the local cache, the adclient process checks the Privilege Control Agent configuration file to see if the user name is mapped to a different Active Directory user account with the adclient.mapuser.username parameter.
   - If the user name is mapped to another Active Directory account in the configuration file, the adclient process queries the Active Directory domain controller or local cache to determine whether the mapped user name has access to computers in the current computer's zone.
7. If the user has a UNIX profile for the zone, the adclient process receives the zone-specific information for the user, such as the user's UID, the user's local UNIX name, the user's global Active Directory user name, the groups of which the user is a member, the user's home directory, and the user's default shell.
8. The adclient process checks for NSS override settings (nss.group.override and nss.user.override) to determine whether there are any changes to the user profile or additional restrictions that should override the profile retrieved or prevent the user from logging on.
9. The adclient process queries through the nss_centrifydc service to determine whether there's another user currently logged in with same UID.
   - If there is a potential conflict between a local user account and the UNIX profile for an Active Directory account, the adclient process notifies the pam_centrifydc service of the potential conflict.
   - The pam_centrifydc service checks the Privilege Control Agent configuration file to determine whether to issue a warning, ignore the conflict, or prevent the user from logging on.
   - If the login continues, the pam_centrifydc service asks the login process for a password.

10. The login process prompts the user to provide a password and returns the password entered to the pam_centrifydc service.
11. The pam_centrifydc service checks the pam.allow.users and pam.deny.users parameters in the agent configuration file to see if any user filtering has been specified to allow or deny access to specific user accounts. If any user filtering has been specified, the current user is either allowed to continue with the login process or denied access.
12. The pam_centrifydc service checks the pam.allow.groups and pam.deny.groups parameters in the agent configuration file to see if any group filtering has been specified to allow or deny access to members of specific groups. If any group filtering has been specified, the current user is either allowed to continue with the login process or denied access based on group membership.
13. If the current user account is not prevented from logging on by user or group filtering, the pam_centrifydc service queries the adclient process to see if the user is authorized to log on.
14. The adclient process queries the Active Directory domain controller through Kerberos to determine whether the user is authorized to log on to the current computer at the current time.
15. 15. The adclient process receives the results of its authorization request from Active Directory and passes the reply to the pam_centrifydc service.
16. The pam_centrifydc service does one of the following depending on the content of the authorization reply:
    - If the user is not authorized to use the current computer or to log in at the current time, the pam_centrifydc service denies the user's request to log on through the UNIX login process.
    - If the user's password has expired, the pam_centrifydc service sends a request through the UNIX login process asking the user to change the password. After the user supplies the password, the login process completes successfully.
    - If the user's password is about to expire, the pam_centrifydc service notifies the user of impending expiration through the login process.
    - If the user is authorized to log on and has a current password, the login process completes successfully. If this is the first time the user has logged on to the computer through the agent, the pam_centrifydc service creates a new home directory on the computer in the location specified in the agent configuration file by the parameter pam.homeskel.dir.

How Failover and Disconnected Access Work

The Privilege Control Agent caches data from Active Directory so that users can log on and perform tasks even if the network or Active Directory server is unavailable, whether because of unexpected connectivity problems, scheduled maintenance, or offline operation of a portable computer. There are several configuration parameters that manage how the agent determines its connectivity to Active Directory, the domain controllers it should attempt to connect to, and the operation of the agent if it is unable to connect to any domain controller.

In most cases, you can set the values for the configuration parameters that control failover and disconnected operation by enabling Privilege Control group policies for a site, domain, or organizational unit. Alternatively, you can set these parameters by editing the /etc/centrifydc/centrifydc.conf configuration file on individual computers.

For an overview of how the agent determines the connection status and locates a domain controller to use, see the following topics:

- Establishing a connection to DNS
- Connecting to the closest domain controller
- Restricting the domain controllers contacted
- Switching to disconnected mode
- Responding to DNS configuration changes
- Connecting to trusted forests and domains

Establishing a Connection to DNS

With each request to Active Directory, the Privilege Control Agent first determines its connection status based on upon the availability of a Domain Name Service domain controller. If a DNS request for a host name takes longer than the number of seconds specified by the adclient.dns.response.maxtime parameter, the agent assumes DNS is down and switches to disconnected mode.

While running in the disconnected mode, the agent does not attempt any more synchronous network communications. Instead, it runs a background thread every 30 seconds to determine when DNS becomes available. The default value for the adclient.dns.response.maxtime is 10 seconds, but this value can be changed by group policy or by editing the /etc/centrifydc/centrifydc.conf file.

Note: If the network is disconnected for a short period of time, but during that time no data is needed from Active Directory, the agent does not switch into disconnected mode. The status only changes if a connection attempt to DNS or to Active Directory through LDAP fails.

Connecting to the Closest Domain Controller

If the initial DNS request for a host name is successful, the Privilege Control Agent attempts to connect to the appropriate domain controller and global catalog for its joined domain using the **site information** found in DNS.

Site information is configured using Active Directory Sites and Services and is defined by subnet. Using the site information, the agent queries DNS for a list of the domain controllers in its site and attempts to connect to the nearest domain controller. It will continue trying to connect to each of the domain controllers in its site based on proximity until it finds a server available. If the agent is unable to connect to any of the domain controllers in its site or if no site information is available, the agent tries to connect to any remaining domain controllers listed in DNS.

Because connection status is determined by an attempt to bind to the Active Directory domain controller using an LDAP call, the adclient.ldap.socket.timeout parameter determines the maximum number of seconds the Privilege Control Agent will wait for a socket connection timeout while binding to the LDAP server. The default value is 5 seconds.

Restricting the Domain Controllers Contacted

If you have a large Active Directory infrastructure or some unreliable subnets, you might want to restrict the domain controllers the agent should attempt to connect to if its primary domain controller becomes unavailable. You can limit the list of domain controllers the agent should attempt to connect to by setting the following property in the centrifydc.conf file:

dns.dc.domain_name: hostname [hostname] ...

where the domain_name is the Active Directory domain name, and the hostname is a fully qualified host name that can be resolved using DNS or the /etc/hosts file.

You can also limit the list of global catalog domain controllers the agent should attempt to connect to by setting the following property in the centrifydc.conf file:

dns.dc.forest_name: hostname [hostname] ...

where the forest_name is the forest root domain, and the hostname is a fully qualified host name that can be resolved using DNS or the /etc/hosts file.

Alternatively, you can use the adclient.server.try.max parameter or Maximum Server Connection Attempts group policy to limit the number of domain controllers the agent will attempt to connect to before switching to disconnected mode, eliminating the need to explicitly list the domain controllers using the dns.dc.domain_name and dns.gc.forest_name parameters. For example, to have the agent try a maximum of three domain controllers, you can set the following property in the centrifydc.conf file:

adclient.server.try.max: 3

Because global catalog and domain controller connections are handled independently, Privilege Control Agent for *NIX can still provide authentication services if the global catalog domain controller is disconnected, as long as another domain controller is available.

Switching to Disconnected Mode

After a connection to a domain controller is established, each subsequent request for information from Active Directory checks the connection status. If a request is made to Active Directory and a response is not received within the number of seconds specified by the adclient.ldap.timeout parameter, that request is retried once. For the second request, the agent will wait up to twice as long for a response. If the second request is not answered within that amount of time, the connection to that specific domain controller is considered disconnected. Once a connection to a specific domain controller is in disconnected mode, a background thread will attempt to reconnect to that domain approximately every 30 seconds. By default, the agent waits 7 seconds for a response to the first request. If the request isn't answered, it retries the request and waits up to another 14 seconds for a response before switching to disconnected mode.

The adclient.ldap.timeout parameter specifies the maximum number of seconds to wait for Active Directory fetch, update, and delete requests to improve the response time when an initial connection attempt fails. A separate parameter, adclient.ldap.timeout.search, specifies the maximum time to wait for search requests. If the search timeout value is not specified, the default is double the adclient.ldap.timeout value. By default, therefore, the agent waits a maximum of 14 seconds for search requests.

The values for these parameters can be adjusted for high load or latency networks by configuring group policies or by editing the /etc/centrifydc/centrifydc.conf file.

Responding to DNS Configuration Changes

The DNS information collected when the agent starts and connects to a domain controller is not cached, and idle connections to Active Directory are dropped after 5 minutes by default. If you make changes in the DNS configuration, those changes are detected the next time the agent needs to reconnect, either because an idle connection has been dropped, or the currently connected domain controller suddenly becoming unavailable.

Connecting to Trusted Forests and Domains

If the Privilege Control Agent establishes a successful connection to the joined domain, it also generates or updates the /etc/krb5.conf file using the domain trust information from the global catalog, and attempts to connect to the

trusted domains or to external forests to find all of the domains that are trusted.

Depending on the trust relationships you have defined, network topology, or firewall requirements, querying external trusted forests can have a significant, negative impact on network performance. You can control whether trusted domains and external forests are queried to establish transitive trusts and cross-forest authentication with the adclient.ldap.trust.enabled parameter. Setting the adclient.ldap.trust.enabled parameter to true indicates that you want the Privilege Control Agent to query trusted domains and forests. Setting this parameter to false disables this feature so that the agent does not connect to any external forests or trusted domains.

If you set the adclient.ldap.trust.enabled parameter to true, you can control the maximum number of seconds to wait when searching for trust information in external forests and other trusted domains with the adclient.ldap.trust.timeout parameter. By default, the agent waits 10 seconds. The search operation is not retried if the request times out, but the request is regenerated approximately once an hour.

If your trusted domains and forests are widely distributed, have slow or unreliable network connections, or are protected by firewalls, you might want to increase the value for this parameter to allow time for the Privilege Control Agent to collect information from external domains and forests.

Preparing to Use Multi-Factor Authentication

This guide is intended for UNIX or Windows administrators who intend to configure multi-factor authentication for computers managed by Privilege Control.

There are two separate scenarios for which you might want to require multi-factor authentication:

- **Login** access to Privilege Control-managed computers.
- As part of a **re-authentication** process so that users who are attempting to use Application, Network, and Desktop rights on Windows machines, or command rights with elevated privileges or in a restricted shell on UNIX machines, must provide a password and another form of authentication before they can execute the selected command.

With these two scenarios in mind, you can configure multi-factor authentication based on user roles or computer roles, for specific applications, or for individual commands. You can also skip multi-factor authentication for applications that do not support it or for other reasons on a case-by-case basis by enabling and applying group policy or by setting configuration parameters.

Authorizing Basic Access

This section describes the basic principles of authorization and how to grant access to Centrify-managed computers using the default predefined rights and role definitions for Linux and UNIX computers. You should review the information in this chapter before creating custom role-based access rights and role definitions.

Checking rights and roles with the dzinfo program

You can also view rights and roles for specific users or the current user by running the dzinfo command-line program on Delinea-managed computers. If you want to use the dzinfo program to view roles and rights for other users, however, you must have root permission.

You can run dzinfo without any arguments to see your own rights and role assignments. The command displays detailed information about your role assignments, the availability for each role assignments, your effective rights, the current audit level, and the specific PAM access, command, and secure shell rights you have been granted.

To see more detailed information, such as the days and times a role is available, you can use the --verbose option. For example, to see detailed information, you could type the following command:

dzinfo --verbose

To view roles and rights for a specific user:

1. Log on or switch to root on a managed computer.
2. Run the dzinfo command for a specific user with the username in the command line.

dzinfo username

For example, to see details about the rights and roles assigned to the user sonya, you could type the following command:

dzinfo sonya

If rights and role assignments have been configured for the specified user, the command displays detailed information about the user's role assignments, the availability of those role assignments, the user's effective rights, the audit level in effect, and the specific rights that have been granted.

You can also use the dzinfo program to test whether a user has the right to run specific commands. For more information about using dzinfo and the dzinfo command line options, see the dzinfo man page.

Testing Command Rights

After command rights have been defined, added to role definitions, and assigned, you can use dzinfo --test "command" to check whether you have permission to execute a specific command. You can use the dzinfo username --test "command" command to check whether a specified user has permission to run a specified command. If you want to use the dzinfo program to view command rights for other users, however, you must have root permission.

To check for command rights, you must enter the complete path to the command and enclose the command in single or double quotes. For example, to test whether the user, qa1 has a command right that allows execution of the id command as root, you could run the following command on a Linux or UNIX computer:

[user1@rh5]# dzinfo qa1 --test "/bin/id"

Depending on the role definition and the user's role assignment, the command might display information similar to this:

Testing: User = qa1 command = /bin/id

User qa1 can run the command as 'root' via dzdo, authentication will not be required, noexec mode is off

Troubleshooting Authentication and Authorization

This chapter describes how to use diagnostic tools and log files to retrieve information about the operation of Privilege Control software and how to identify and correct problems within your environment.

Diagnostic tools and log files

All Delinea services include diagnostic tools and logging mechanisms to help you trace the source of problems if they occur. These diagnostic tools and log files allow you to periodically check your environment and view

information about Delinea operation, your Active Directory connections, and the configuration settings for individual UNIX and Linux computers.

Although logging is not enabled by default for performance reasons, log files provide a detailed record of Delinea Agent (adclient) activity. This information can be used to analyze the behavior of adclient and communication with Active Directory to locate points of failure. However, log files and other diagnostic tools provide an internal view of operation and are primarily intended for Delinea experts and technical staff.

In most cases, you should only enable logging when you need to troubleshoot unexpected behavior, authentication failure, or problems with connecting to Active Directory or when requested to do so by Delinea Support. Other troubleshooting tools, such as command line programs, can be used at any time to collect or display information about your environment.

Logging to the circular in-memory buffer

If the Delinea Agent for *NIX's adclient process is interrupted or stops unexpectedly, a separate watchdog process (cdcwatch) automatically enables an in-memory circular buffer that writes log messages passed to the logging subsystem to help identify what operation the adclient process was performing when the problem occurred. The in-memory buffer is also mapped to an actual file, so that if there's a system crash or a core dump, the last messages leading up to the event are saved. Messages from the in-memory circular buffer have the prefix _cbuf, so they can be extracted from a core file using the strings command.

The in-memory circular buffer allows debug-level information to be automatically written to a log file even if debugging is turned off. It can be manually enabled by restarting the adclient process with the -M command line option. The default size of the buffer is 128K, which should be sufficient to log approximately 500 messages. Because enabling the buffer can impact performance, you should not manually enable the circular buffer or modify its size or logging level unless you are instructed to make the changes by Delinea Support.

Collecting Diagnostic Information

You can use the adinfo command to display or collect detailed diagnostic and configuration information for a local UNIX computer. Options control the type of information and level of detail displayed or collected. The options you are most likely to use to collect diagnostic information are the --config, --diag, or --support options, which require you to be logged in as root. You can redirect the output from any adinfo command to a file for further analysis or to forward information to Delinea Support.

For more information about the options available and the information returned with each option, see the man page for adinfo.

To display the basic configuration information for the local UNIX computer, you can type:

adinfo

If the computer has joined a domain, this command displays information similar to the following:

Local host name: magnolia

Joined to domain: ajax.org

Joined as: magnolia.ajax.org

Current DC: ginger.ajax.org

Preferred site: Default-First-Site-Name

Zone: ajax.org/Ajax/Zones/corporate

Last password set: 2006-12-28 14:47:57 PST

CentrifyDC mode: connected

Licensed Features Enabled

Working with Domain Controllers and DNS servers

Delinea Agents are designed to perform the same set of DNS lookup requests that a typical Windows workstation performs to find the nearest domain controller for the local site. The DNS lookup request enables the Delinea Agent for *NIX to find domain controllers as they become available on the network or as the computer is relocated to another network location where different domain controllers are present. Delinea Agents also use DNS to find the Kerberos service providers and the global catalog service providers for the Active Directory forest.

In a typical Windows environment, the DNS server role is updated dynamically to contain the service locater (SRV) DNS entries for Active Directory's LDAP, Kerberos, and global catalog services, so this information is available for Delinea Agents to use. However, there are some configurations of DNS that might not provide all of the SRV records for the set of domain controllers that provide Active Directory service to the enterprise. You may also run into problems if DNS for the enterprise runs on UNIX servers that cannot locate your Active Directory domain controllers. The next sections describe how you can adjust DNS or Delinea Agent to ensure they work together properly in your environment.

Configuring the DNS Server Role on Windows

One of the most common scenarios for running DNS in an environment with Active Directory is to add the DNS server role to a Windows domain controller or another Windows server.

If you are already using DNS in Active Directory and dynamically publishing DNS service records, no additional configuration should be necessary. If you are using DNS in Active Directory but have disabled dynamic updates, you should change the configuration for the DNS server role to allow dynamic updates. Making this change will allow Delinea Agents to properly locate domain controllers in the site and select an appropriate new domain controller if a connection to its primary domain controller is lost or the managed computer is moved to a new location on the network.

Configuring DNS Running on UNIX Servers

If your environment is configured to use UNIX-based DNS servers instead of Active Directory-based DNS servers and the UNIX system is configured to use DHCP, the nameserver entry in /etc/resolv.conf file is set automatically to point to a DNS server.

If this DNS server is aware of the Active Directory domain you want to join, no further changes are needed. If the DNS server identified as a nameserver in the /etc/resolv.conf file is not aware of the domain you are trying to join, for example, because you are using a test domain or a separate evaluation environment, you need to either disable DHCP or manually set the location of the Active Directory domain controller in the Delinea configuration file.

Checking whether DNS can Resolve the Domain Controller

In most cases, you can verify whether a UNIX computer can locate the domain controller and related services by running the ping command and verifying connectivity to the correct Active Directory domain controller or by checking the nameserver entry in the /etc/resolv.conf file. This nameserver entry should be the IP address of one of the domain controllers in the domain you want to join.

If the ping command is successful, it indicates the DNS server is aware of the Active Directory domain you want to join, and no further changes are needed. If the ping command is not successful, you will need to take further action to resolve the issue.

Resolving Issues in Locating Active Directory Domain Controllers

If the UNIX computer cannot find the Active Directory domain controller, there are several ways you can resolve the issue. Depending on your environment and specific situation, you should consider doing one of the following:

- Set up DNS on the target Active Directory domain controller and the manually configure the nameserver entry in the /etc/resolv.conf file to use that domain controller as described in the next section, *Setting up DNS service on a target domain controller*.
- Set the Delinea configuration file to manually identify the domain controllers you want to use as described in the section below, *Setting the domain controller in the configuration file*.

Setting up DNS Service on a Target Domain Controller

One of the simplest ways to ensure that the UNIX computers can locate the Active Directory domain controller and related services is to use the DNS service on the Active Directory domain controller as a DNS slave to the enterprise DNS servers. You can do this is by configuring the DNS server role on the Active Directory domain controller, then specifying that domain controller in the UNIX computer's /etc/resolv.conf file. You can then add a forwarder to the local DNS on the domain controller that will pass on all lookups that it cannot satisfy to an enterprise DNS server.

This configuration does not require any changes to the enterprise DNS servers. Any look up request from the domain controller is simply a query from another computer in the enterprise. However, the UNIX computers configured to use this slave DNS service will receive the appropriate Service Location (SRV) records and global catalog updates for the Active Directory domain controller. In addition, the DNS service on the domain controller can be configured to forward requests to the enterprise DNS servers so those requests can be answered when the local DNS service cannot respond.

Adding a DNS Server Role to an Active Directory Domain Controller

The specific steps for adding the DNS server role to a domain controller depend on the version of Windows Server you use. In most cases, you can use an administrative tool, such as Server Manager, to add roles. Follow the instructions displayed in the wizard to add the DNS Server server roles, configure the DNS server lookup zones, select the Allow both nonsecure and secure dynamic updates option.

After you have configured the DNS server role on the domain controller, the computer uses the local DNS server as its primary DNS server.

Configuring UNIX to use DNS service on the target domain controller

Once you have configured the DNS service to contain the required Active Directory entries, you simply need to modify the UNIX computer to send all DNS lookup requests to the newly configured DNS server.

To configure the UNIX computer to use the new DNS server:

1. Open the /etc/resolv.conf file.
2. Set the IP address of the nameserver entry to the IP address of the DNS server on the Active Directory domain controller you just configured.

Setting the domain controller in the configuration file

If you are not able to use DNS to locate the Active Directory domain controllers on your network, you can manually specify one or more domain controllers in the Delinea configuration file.

To manually specify a domain controller, add the following entry to the Delinea configuration file, /etc/centrifydc/centrifydc.conf:

dns.dc.domain_name: server_name [server_name ...]

For example, if you want to ensure the Delinea Agent uses the domain mylab.test and the domain controller named dc1.mylab.test, you could add the following line to the /etc/centrifydc/centrifydc.conf file:

dns.dc.mylab.test: dc1.mylab.test

Note: You must specify the name of the domain controller, not its IP address. In addition, the domain controller name must be resolvable using either DNS or in the local /etc/hosts file. Therefore, you must add entries to the local /etc/hosts for each domain controller you want to use if you are not using DNS or if the DNS server cannot locate your domain controllers.

To specify multiple servers for a domain, use a space to separate the domain controller server names. For example:

dns.dc.mylab.test: dc1.mylab.test dc2.mylab.test

The Delinea Agent will attempt to connect to the domain controllers in the order specified. For example, if the domain controller dc1.mylab.test cannot be reached, the agent will then attempt to connect to dc2.mylab.test.

If the global catalog for a given domain is on a different domain controller, you can add a separate dns.gc.domain_name entry to the configuration file to specify the location of the global catalog. For example:

dns.gc.mylab.test: dc3.mylab.test

You can add as many domain and domain controller entries to the Delinea configuration file as you need. Because the entries manually specified in the configuration file override any site settings for your domain, you can completely control the Delinea Agent for *NIX's binding to the domains in your forest through this mechanism.

Note: In most cases, you should use DNS whenever possible to locate your domain controllers. Using DNS ensures that any changes to the domain topology are handled automatically through the DNS lookups. The settings in the configuration file provide a manual alternative to looking up information through DNS for those cases when using DNS is not possible. If you use the entries in the configuration file and the domain topology is changed by an Active Directory administrator, you must manually update the location of the domains in each configuration file.

Using the fixdns script

The Delinea Agent includes a fixdns script that you can use to inspect your environment and make the necessary configuration file changes for you.

To run this script, you need to specify the domain controller name and IP address:

fixdns domain_controller_name IP_address

For example, if you intend to join the domain mytest.lab and the domain controller for that domain is dc1.mytest.lab and its address is 172.27.20.1, you would run the following command:

fixdns dc1.mytest.lab 127.27.20.1

The fixdns script will then make the necessary changes to the /etc/hosts and the Delinea configuration file.

Note: This script does not update the /etc/resolv.conf file. If the script cannot locate the domain controller using the existing /etc/resolv.conf settings, it will assume that you want to use settings from the configuration file.

What the Privilege Control DNS Subsystem Provides

Privilege Control provides a DNS subsystem that bypasses the local DNS resolver to address common issues that occur with many local DNS resolvers. These common issues for local DNS resolvers include:

- Degraded performance when connecting to a slow DNS server or when attempting to use dead DNS servers.
- Degraded performance when reacquiring a DNS server that went offline and has come back online.
- Degraded performance related to DNS timeouts.
- Platform-related DNS idiosyncrasies, such as MDNS, appending.LOCAL suffixes, and so on.

The Delinea DNS subsystem performs the following functions:

- Looks up hosts by name.
- Looks up hosts by IP address.
- Queries DNS service location records (SRV) to discover the domain controllers that support Active Directory services including KDC, KPASSWD, LDAP and the global catalog.

Resolving a host name or IP address

When the DNS client subsystem receives a DNS requests, it attempts to resolve the host name or IP address by first checking the /etc/hosts file. If the file contains a valid entry to resolve the specified host name or IP address, the DNS client subsystem processes the DNS request.

Entries in /etc/hosts must be in the following format:

IPv4_address hostname alias alias ...

where:

- IPv4_address must be in the first position
- hostname is a fully qualified domain name and must be in the second position.
- aliases are optional and follow the address and hostname entries.

For example:

192.169.147.135 ginger.acme.com ginger

Note: Service (SRV) record queries cannot be satisfied from the /etc/hosts file.

If resolution by /etc/hosts is unsuccessful, the DNS subsystem attempts to select a DNS server that can be used to resolve the host name or IP address as described in the next section.

Selecting a DNS server

If unable to resolve a host name or IP address by finding an entry in the /etc/hosts name (as described above in *"Resolving a host name or IP address" on the previous page*), the Delinea DNS subsystem attempts to find a DNS server to resolve the host name or IP address, as follows:

- It checks for a working DNS server that has already been selected (cached in memory and stored in /var/centrify/kset.dns.server), and if available, uses it.
- If a working DNS server is not already selected, it checks /etc/resolv.conf for configured DNS servers, and if populated, selects the fastest one from the list.

If no working DNS servers are found, the request fails.

At this point, DNS is considered down, and the Delinea DNS subsystem waits for the interval specified by the dns.dead.resweep.interval (default is 60 seconds), before attempting again to find a DNS server.

Specifying DNS-related parameters

Parameters in the Delinea configuration file control many aspects of Delinea DNS subsystem operation. Although you can set any of these parameters, the default settings should provide you with optimal DNS operation. See the Configuration and Tuning Reference Guide for details about any of these parameters.

The DNS subsystem periodically checks in the background to see if a DNS server that is faster than the currently selected one is available. The dns.alive.resweep.interval parameter determines how often this background check occurs; the default value is one hour (3600 seconds).

When a DNS server is selected, its address is stored in the kset.dns.server file, and it is used for all DNS requests until one of the following occurs:

- The selected server stops responding.
- A new server sweep discovers a faster DNS server and replaces it.
- The adclient process is stopped and restarted, which triggers a sweep for a new DNS server.
- The specified server is no longer in the list of servers in /etc/resolv.conf.

For the sweep, the dns.sweep.pattern parameter determines the probe pattern that is used to find a live DNS server; that is, it sets the protocol to use (TCP or UDP) and the amount of time to wait for a response. By default, this parameter specifies both a TCP and UDP probe.

The dns.timeout and dns.udp.retries parameters determine the amount of time to wait, and how often to re-send a request when the current server does not respond to a request. If the current server does not respond to a request within the specified time out period, it is considered down and Delinea looks for a different server. If it cannot find a live server, DNS is considered down, and the Privilege Control Agent for *NIX waits for the period of the dns.dead.resweep.interval parameter, 60 seconds by default, before performing a sweep to find a new server.

Filtering the objects displayed

For performance or security reasons, you might want to filter or limit the objects displayed in the Access Manager console. Depending on your environment, you might want to display more or less information by setting filter

options. These filter settings enable you to control both the number and type of objects displayed. You should note, however, that these settings can affect the performance of the console.

To filter the objects listed in Access Manager:

1. Open Access Manager.
2. In the console tree, select **Access Manager**, right-click, then click **Options**.
3. Click the **Filter Settings** tab.
4. Select **Load all zones** to automatically open either all zones in the connected forest or all zones in a specific parent container.
   - If you select this option and **connected forest** all zones in the forest are opened automatically each time you start Access Manager.Selecting this option prevents you from opening or closing any zonesmanually. Depending on the number of zones you have, you might experience slower performance in the console if you select this option.
   - If you select this option and **container**, you can then click Browse to search for a container from which to automatically load zones.Selecting this option prevents you from opening or closing any zones manually. Depending on the number of zones you have in the selected container, you might experience slower performance in the console if you select this option.
5. Select **Show disabled Active Directory accounts** to display disabled computer and user accounts or uncheck this option to hide disabled objects.
6. Select **Show orphans** to display all users, groups, and computers that have a UNIX profile or uncheck this option to hide all orphan profiles.
   Orphan profiles are the service connection points that no longer have a corresponding Active Directory object. Hiding or removing orphan profilescan improve console performance.
7. Select **Show Auto Zone** to display the users, groups, and computers that have joined the Auto Zone or uncheck this option to hide Auto Zone information.
8. Set the **Maximum number of items to be displayed in the list** option to limit the total number of objects displayed in the console, up to total maximum allowed (65535).
9. This setting applies to all of the objects displayed in Access Manager, including zones, computers, users, groups, pending users, pending groups, NIS maps, and all defined rights, roles, and role assignments. Lowering the maximum number of items displayed improves performance when browsing the listed items. Note that this setting does not affect the number of items you can define, only the number displayed.
10. Click **OK.**

Using Use My Account

Note: Consider moving content here from the Setting Up Training doc.

Installing Agents on Computers to be Managed

This section describes the recommended steps for deploying Privilege Control software on the nonWindows computers that you want to add to Active Directory. The chapter 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.

About the Deployment Process

There is no technical requirement that you only work with a subset of computers at a time, but in practice 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.

Select a Target Set of Computers

As a first step in preparing to install Privilege Control software, you should 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

You can:

- 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.

Install 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 on or switch to the root user if you are installing on a Linux or UNIX.
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, which could be in tgz or tar format. 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.

Install 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 Available

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, you should 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, you can set the following parameters:

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_ldapproxy="K" Note that these additional packages may have dependencies or require a specific version of the Privilege Control Agent for *NIX to be installed. Before installing or updating additional packages silently, you should review the information in the Upgrade and Compatibility Guide. | 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:

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. Note that the install.sh script calls adcheck twice. After the first call, adcheck 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 adcheck 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 skipped. Set this parameter to Y if you want to run adcheck 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.
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 install.sh 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.

Parameter	Description
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.
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.

Parameter	Description
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.
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.

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_ldapproxy=”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

Use 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, etc, 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 agent package for platform-specific installation details.

About the Files And Directories Installed on the Agent

When you complete the installation, the local computer will be updated with the following directories and files for the core Privilege Control Agent for *NIX:

This directory	Contains
/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.

This directory	Contains
/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, that is, 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 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.

Identity Threat Protection and Privilege Control for Cloud Entitlements

On the Delinea Platform, 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.

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 is sometimes referred to as Identity Threat Detection and Response (ITDR).

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 offboarding 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, via easy integrations with SIEM, SOAR, and XDR solutions to ensure standard procedures in handling identity and access incidents.

Privilege Control for Cloud Entitlements (PCCE)

Privilege Control for Cloud Entitlements reduces access risks across multi-cloud infrastructure by controlling privilege sprawl. PCCE is sometimes referred to as Cloud Infrastructure Entitlement Management (CIEM). 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/PCCE

For instructions on setting up ITP/PCCE, follow the relevant link or links below:

- Integrating AWS with 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 Delinea Platform (PCCE)
- Integrating Entra ID & Azure Cloud with Delinea Platform (ITP/PCCE)
- Integrating Okta with Delinea Platform (ITP)
- Integrating PingOne with Delinea Platform (ITP)

Inventories

For both Identity Threat Protection and Privilege Control for Cloud Entitlements, Inventories provides 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.
- **Automate User Access Reviews**: With comprehensive inventories, organizations can automate user access reviews across their cloud environment to ensure attestation and compliance.

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 accounts and users without MFA.
- Define dynamic scopes 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

Inventories are displayed on the following pages:

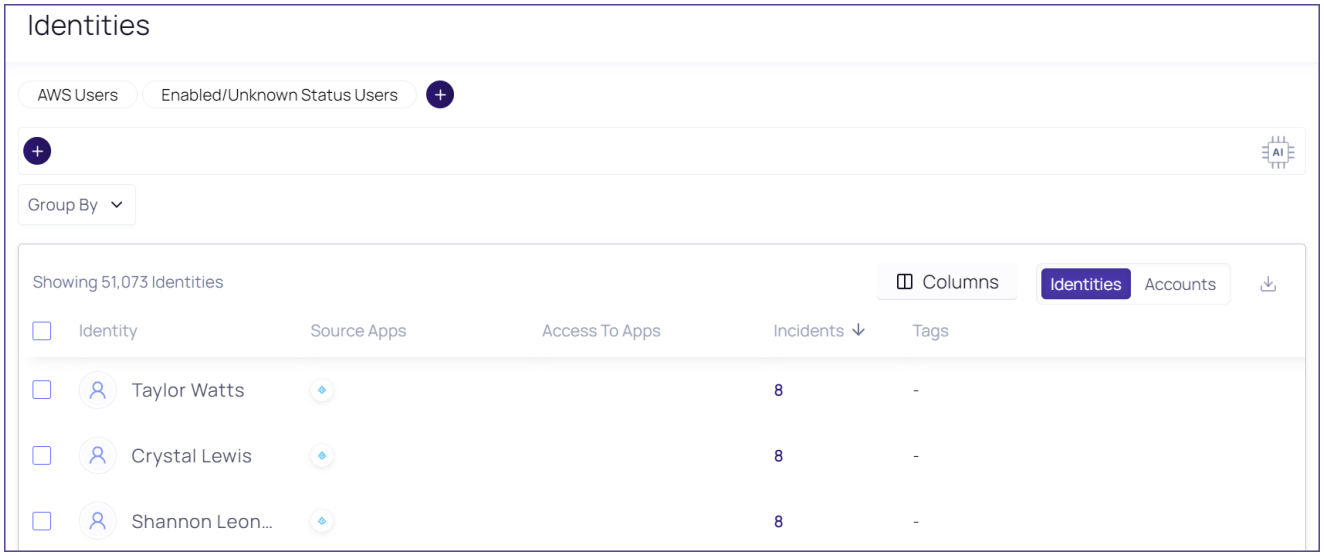
- **Identities**: Displays identities and accounts
  - **Identity**: A unique identity (human or nonhuman) that owns one or more accounts. A nonhuman identity could be a machine identity, an automatic identity, or any other identity that doesn't belong to a human.

- **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 "group" permissions 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 R&D department, the Membership inventory will present 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 (group or user) and an asset.
- **Privileges**: Displays a list of all privileges at all levels.
- **Activities**: Displays who did what, and when it was done.

Inventories User Interface

You can access inventories by clicking **Inventory** from the left navigation menu, then selecting one of the choices from the secondary menu such as Identities. The Identities page is shown in the screen shot.



Filter the 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 environment as well as their current status.

For example, you can display all the identities with admin privileges whose accounts were disabled or suspended (or are unknown).

The filter fields for each inventory are described in "Inventory Filter Properties" on page 502.

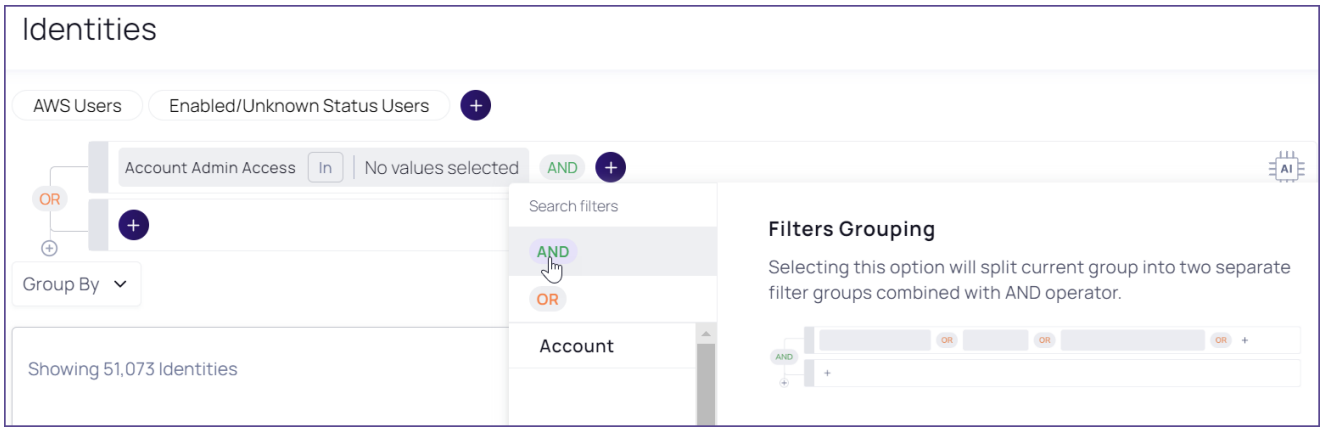
If you have imported custom properties (shown at the end of the list), you use those to filter. For more information on importing custom properties, see "Search by custom properties" on the next page.

You can use these filter methods in the inventories:

- **Basic filter** (Identities, Groups, Assets, and Privileges inventories). Filter the inventory table based on that inventories' properties.
- **Advanced filter** (Memberships, Access Policies, and Activities inventories). Filter an inventory table based on a broader set of properties as well as on the interconnected relationships and paths within the system. For example, you can filter for both actor and target.

Filter lines are connected by all AND operators or by all OR operators.

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



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

You can also enter human-readable text (such as, "show me admins without MFA"). Click AI then type search text, then click **Ask AI**.

On many inventory pages, you can choose among predefined quick filters that are commonly used for that inventory.

To filter a table:

- To add filter fields, click **+** and select from the available filter fields.
- To remove fields, hover over a field and click **X**.

The table is filtered on the fly.

Inventory filters support the following operands:

- Exact matches
  - In or Not In
  - Is Empty
- Mathematical matches
  - Equal to, Greater than, etc.
- Date matches
  - Yesterday, Last Week, Last Year, Custom, etc.
- String matches
  - Contains or Not contains
  - Ends with or Not Ends with
  - Starts with or Not Starts with

Regardless of how they were added, the properties can be searched in the relevant inventory.

Search by custom properties

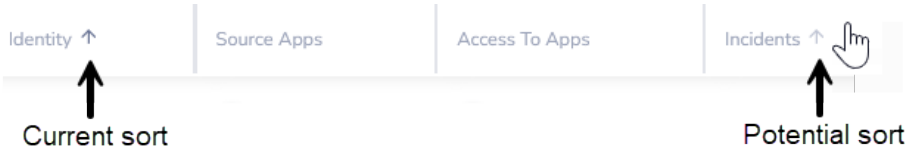
You can search by custom application properties, such as subscriptions in Azure or public repositories in GitHub or GitLab. This enables you to better scope the results, based on your unique organizational values.

Custom properties are added by:

- **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.

Sort the inventory table

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



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.

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), and you can easily investigate 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.

Configure table columns

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

- Which columns are displayed
- Column width
- Column order

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 grey column dividers on both sides are displayed.
2. Drag and drop the column.

Export the table as CSV

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

Use tags

Tags are keywords (“metadata”) attached to data to enable that data to be found by browsing or searching.

Tags are displayed on the inventory tables, and in the single-entity view. Tag names are usually self-explanatory, and you can hover your cursor over system tags 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 the inventory pages (not from the Membership or Access Policies pages) or from the single-entity view. These can be existing tags or new tags that you create on the fly.

You can apply tags to one or multiple entities simultaneously.

To apply existing or new tags from an inventory page

1. Select the row to tag.
   To apply the same tag to multiple rows, select multiple rows.
2. Click **Add Tags**, then click **Add tags**.
3. To apply an existing tag, select the tag, then click **Save**.
   You can search for tags by typing the first few letters.
4. To create a new tag, do this:
   a. Type a new tag name.
   b. Click **Add New**.
   c. To apply the new tag, click **Save**.
      If you do not apply the tag, the new tag is created and can be applied to entities later.

You can apply both existing and new tags in the same step.

To create new tags

1. Select an inventory row.
2. Click **Add Tags**, then click **Add tags**.
3. Type a new tag name.
4. Click **Add New**.
5. To add more new tags, type a new tag name and click **Add New**.

Inventory Filter Properties

Identities

Category	Property	Description
Account	Access To Apps	The applications a user (or service account) can access. The access might be direct or indirect (such as federated access).
	Admin Access	The Admin filter enables you to find user accounts with administrative privileges. You can specify the application for which you want to find users with admin access. To modify this setting, navigate to the Settings page > Authorization Configuration.
	Blast Radius Risk	The blast radius presents the impact of an account to be taken over, based on the account's access and type of access.

Category	Property	Description
	Email	Email of the user (or service account) as found in the application.
	First Name	First name of the 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 (e.g. the incidents in the AWS account).
	Is External	"Is the account external? (Yes or No) External accounts are based on the email and properties of the account being different from internal users (or as stated in the downstream application)."

Category	Property	Description
	Is Managed	A managed account is managed by the current system's admin, meaning that as an admin, you can disable the account. Use this filter to find all accounts your admins have full control over, or those they do not control that have access to your systems.
	Is MFA Enabled	Is MFA set in this application? (Yes or No) MFA settings may be different in different accounts, so 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 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 Account takeover risk (the probability for an account to be taken over) and the blast radius (the impact)
	Detection Rule Name	The filter enables you to filter based on users who match a specific detection rule, for example finding all the users that matched the brute force attack.
	Privileged Access	The Privileged filter enables you to find user accounts with privileged access. You can select the application to identify users with privileged access. To modify this configuration, go to the Settings page > Authorization Configuration.

Category	Property	Description
	Shadow Admin Access	The Shadow-Admin filter enables you to find 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 user. For example, if a user has federated access to AWS via his IDP (e.g. Okta) then Okta is the source app, and AWS is found in the Access to app filter.

Category	Property	Description
	Status	The status of the account in the source application, such as Deleted, Disabled, Enabled, or Unknown.
	Sub Type	The sub-type filter present all the available sub-types of non-human Identities.
	Tags	Tags that are associated with the account (e.g. 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 account takeover risk presents the probability that an account will be taken over by an external identity
	Type	User or Service Account

Category	Property	Description
Dynamic Scope	Name	The named Dynamic Scope is used as a filter. All dynamic scope types can appear in the filter. If an Access-type scope is used, then the identities that matched will be returned.
Identity	Blast Radius Risk	The Identity Blast Radius filter helps you identify identities based on the risk imposed by their access scope. It 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 users with extensive access permissions, enabling you to prioritize security measures and reduce the overall risk of breaches.

Category	Property	Description
	Department	The department in which the identity works (e.g. Bus Dev., Customer Support, Sales, HR…).
	First Name	The first name of the identity is 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 name from the Primary account.

Category	Property	Description
	Overall Risk	The Identity Overall Risk filter allows you to evaluate the comprehensive risk of an identity by considering the combined risks of its individual accounts. It 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. By utilizing this filter, you can easily search for identities with significant security concerns, prioritizing measures to mitigate potential breaches and safeguard sensitive data.

Category	Property	Description
	Source Apps	Source Apps represents all applications for which the identity has a registered user account. For example, if a user has federated access to AWS via his IdP (for example Okta) then 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 (e.g. Senior Employee, Involved in Credential leak, Finance Employee). Tags are created automatically by the AI engine or manually by the end user.

Category	Property	Description
	Take Over Risk	The Identity Account Takeover Risk filter evaluates the ease with which an attacker could gain access to any of an identity's connected accounts. It 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 proactively identify identities with weak account security, allowing you to prioritize security enhancements and protect against potential unauthorized access and data breaches.
	Terminated At	Terminated At
	Title	The job title of the identity (e.g. CTO, SW Engr. for example)

Groups

Category	Property	Description
Group	Admin Access	The Admin filter enables you to find user accounts with administrative privileges. You can specify the application for which you want to find users with admin access. To modify this setting, navigate to the Settings page > 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
	Dynamic Scopes	The named Dynamic Scope is used as a filter. Filtering is based upon the results of the dynamic scope in this inventory, so the results will be all the groups that matched the Dynamic Scope.
	ID	ID
	Incidents Counts	The named Dynamic Scope is used as a filter. Filtering is based upon the results of the dynamic scope in this inventory, so the results will be all the groups that matched the Dynamic Scope.
	Is Empty	Filters for 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.
	Detection Rule Name	The filter enables you to filter based on groups who matched a specific detection rule, for example finding groups that grant admin access.
	Privileged Access	The Privileged filter enables you to find user accounts with privileged access. You can select the application to identify users with privileged access. To modify this configuration, go to the Settings page > Authorization Configuration.

Category	Property	Description
	Shadow Admin Access	The Shadow-Admin filter enables you to find 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 (general, birthright group for example). Tags are created automatically by the AI engine, manually by the end user, or are based on the tags in the source system.

Assets

Category	Property	Description
Asset	Created At	Creation date of the asset, if available.
	Dynamic Scopes	The named Dynamic Scope is used as a filter. Filtering is based upon the results of the dynamic scope in this inventory, so the results will be all the Assets that matched the Dynamic Scope.
	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 in Asset of Type Secret or of type 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	The filter enables you to filter based on assets that matched a specific detection rule, for example finding production assets that can be accessed by non-admins.
	Source App	The app on which the asset is managed.

Category	Property	Description
	Tags	Tags associated with the asset (Production or Test Environment for example).
	Type	Assets are "normalized" (grouped) to a minimal set of types across all applications. Consequently, assets can 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	
	Identity	Dynamic Scope	Same as Identities-Dynamic Scope	
	Identity	Identity	Same as Identities-Identity	
	Group	Group	Same as Groups inventory	
Target	Group	Group	Same as Groups inventory	
Access		Membership	Added at	Filter when this membership was created.
			Added by	Filter by whom this membership was created.
			Direct Access	Direct Access
			Dynamic Scopes	Dynamic Scopes

Access Policies

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities-Account	
	Identity	Dynamic Scope	Same as Identities-Dynamic Scope	

Filter	Entity Type	Category	Property	Description
	Identity	Identity	Same as Identities-Identity	
	Group	Group	Same as Groups	
Target	Asset	Asset	Created At	Creation date of the asset, if available.
			Dynamic Scopes	The named Dynamic Scope is used as a filter. Filtering is based upon the results of the dynamic scope in this inventory, so the results will be all the Assets that matched the Dynamic Scope.
			ID	ID
			Incidents Count	The number of incidents associated with the asset.

Filter	Entity Type	Category	Property	Description
			Last Used At	The last time the asset was used (accessed, modified, deleted or created). This data is available mainly in Asset of Type Secret or of type 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	The filter enables you to filter based on assets that matched a specific detection rule, for example finding production assets that can be accessed by non-admins.

Filter	Entity Type	Category	Property	Description
			Source App	The app on which the asset is managed.
			Tags	Tags associated with the asset (Production or Test Environment for example).
			Type	Assets are "normalized" (grouped) to a minimal set of types across all applications. Consequently, assets can 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	Dynamic Scopes	The named Dynamic Scope is used as a filter. Only access-type dynamic scopes will yield results in this inventory

Filter	Entity Type	Category	Property	Description
			Granted at	Filter when this access policy was created.
			Granted by	Filter by whom this access policy was created.
			Is Direct	A direct assignment of access is any access granted to the account/group directly and not via another group. when marked as Yes only direct access will be shown and calculated in the result, if marked as not only indirect will be included, for both options remove or do not use the filter at all.
			Last Used At	Filter access policies by their last used date.

Filter	Entity Type	Category	Property	Description
			Limit Inheritance	The filter will only include the first asset in the system that matches the query and will not return any inherited assets. For example, if you are asking to find administrative access in a file system and a user has access to a folder and the folder has a file, by applying this filter the result will only include the folder.
		Privilege	Is Role	Filter on the privileges of a role on different assets. In other words, 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	Use this filter to find a privilege that contains a specific child privilege, for example, search the privilege add MFA and find every admin or similar roles/privileges that can add MFA devices
	Is Role	Does the privilege represent a role on the application? (Yes or No).
	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 (Production or Test Environment for example).
	Type	Privileges are "normalized" (grouped) to a minimal set of types across all applications. Consequently, privilege can 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).

Activities

Filter	Entity Type	Category	Property	Description
Actor	Identity	Account	Same as Identities-Account	
	Identity	Dynamic Scope	Same as Identities-Dynamic Scope	
	Identity	Identity	Same as Identities-Identity	
	Group	Group	Same as Groups	
Target	Asset	Asset	Same as Access Policies Target Asset	
	Identity	Account	Same as Identities-Account	
	Identity	Dynamic Scope	Same as Identities-Dynamic Scope	
	Identity	Identity	Same as Identities-Identity	
	Group	Group	Same as Groups	

Filter	Entity Type	Category	Property	Description
Privilege		Privilege	Child Privileges	Use this filter to find a privilege that contains a specific child privilege, for example, search the privilege add MFA and find every admin or similar roles/privileges that can add MFA devices
			Is Role	Does the privilege represent a role on the application? (Yes or No).
			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 (Production or Test Environment for example).

Filter	Entity Type	Category	Property	Description
			Type	Privileges are "normalized" (grouped) to a minimal set of types across all applications. Consequently, privilege can 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).
Activity		Activity	Date	The date when the activity was performed.
			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

The Identities inventory table shows the following:

- **Identities**: A unique identity (human or nonhuman) that owns one or more accounts. A nonhuman 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 nonhuman) in a single application. A nonhuman account might be a service account, a workload, or even a user account used for automated tasks.

You can view the Identities page from **Inventory** > **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, contact Customer Support.
- 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.

Filter and modify the table display

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 dynamic scope 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

These filter and display options are described in full in "Inventories User Interface" on page 497.

You can also investigate an entity in Access Explorer, by clicking , as described in "Access Explorer" on page 534.

Insight into selected 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 will be shown in the Source Apps column and all the apps that can be accessed (via Okta) will be shown in the Access to app column.

Insight into selected filter options

- To focus on federated apps, use Account Source App to filter for the federated apps you are interested in.
- You can 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 these 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**.

Groups

The Groups inventory table shows all entities that "group" 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 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.

You can view the Groups page from **Inventory** > **Groups**.

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.

Filter and modify the table display

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
- The full list of filters is described in Inventory Filter Properties.
- save a filter as a dynamic scope 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 a group by displaying its single-entity view

These filter and display options are described in full in Inventories User Interface.

You can also investigate an entity in Access Explorer, by clicking , as described in "Access Explorer" on page 534.

Insight into selected table data

- 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.

Alternative Names

To provide additional information to users reviewing groups, you can add an alternative name to a group via 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

Assets are objects monitored by the platform that you can govern, for example: file/folder, database, virtual machine, application. Assets can be accessed from the Inventory menu.

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 incidents are open about it, and the associated tags.

If a table in any of the pages becomes excessively large, you can focus your display with the help of search and filters.

The Assets Page

You can view the Assets page from **Inventory** > **Assets**.

The Assets page opens to display all the identities in your organization. You can see how many Assets you have, how many Incidents are opened in their name, and Identity Tags.

Filter and modify the table display

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. The full list of filters is described in Inventory Filter Properties.
- save a filter as a dynamic scope 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 a group by displaying its single-entity view

These filter and display options are described in full in "Inventories User Interface" on page 497.

You can also investigate an entity in Access Explorer, by clicking , as described in "Access Explorer" on page 534.

Insight into selected table data

- The Type column displays the platform “normalized” type name (e.g. all types of databases are referred to as “database”).
- The Origin Type column displays the type names from the original product (e.g. 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.

You can view the Memberships page from **Inventory** > **Memberships**.

By default, the Memberships inventory table is sorted by number of incidents, in descending order.

Filter and modify the table display

To customize the table view, you can:

- filter the content displayed. The full list of filters is described in "Inventory Filter Properties" on page 502.
- save a filter as a dynamic scope 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
- zoom in on an entity by displaying its single-entity view
- see a quick view of an entity

These filter and display options are described in full in "Inventories User Interface" on page 497.

You can also investigate an entity in Access Explorer, by clicking , as described in "Access Explorer" on page 534.

Insight into selected filter options

You can filter the results 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 table, Identities filter category, in Inventory Filter Categories.
- **Target**: Click **+** to select a specific group. The filters are the same as those described in the Groups filter table, in Inventory Filter Categories.
- **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 access to a specific asset with a specific permission.

There are two main types of access policies:

- **Grouping** - things that group accounts or other groupings together
- **Permission** - things that grant A access to B with privilege Y

Examples:

- a group through which someone gains access to something
- a direct access to a resource with certain privileges
- assignment to a role in AWS
- the profile assigned to a user in Salesforce (SF Profile=Group)

You can view the Access Policies page from **Inventory** > **Access Policies**.

Filter and modify the table display

To customize the table view, you can:

- filter the content displayed. The full list of filters is described in "Inventory Filter Properties" on page 502.
- save a filter as a dynamic scope 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
- zoom in on an entity by displaying its single-entity view
- see a quick view of an entity

These filter and display options are described in full in "Inventories User Interface" on page 497.

Privileges

A privilege is anything 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 platform.

You can view the Privileges page from **Inventory** > **Privileges**.

By default, the Privileges inventory table is sorted by name, in ascending order.

Filter and modify the table display

To customize the table view, you can:

- filter the content displayed. The full list of filters is described in "Inventory Filter Properties" on page 502.
- change the sort order
- change the display of columns
- use tags
- zoom in on an entity by displaying its single-entity view

These filter and display options are fully described in "Inventories User Interface" on page 497.

Insight into selected filter options

You can filter using these 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**: if 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, like creating a virtual machine, segmented by create, read, update, detect.

Privileges 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.

You can view the Activities page from **Inventory** > **Activities**.

By default, the table shows activity from the past week that is nonvirtual.

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 will show only those activities in the timeframe represented by the bar.

Filter and modify the table display

By default, the Activities inventory table is sorted by date, 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.
- change the sort order
- change the display of columns
- use tags
- zoom in on an entity by displaying its single-entity view
- see a quick view of an entity

These filter and display options are fully described in Inventories User Interface.

You can also view the raw log of the activity as it was fetched from the system of origin, by clicking on the raw log icon at the end of the table row or on the side panel displayed when clicking on the row.

Dynamic Scopes

Dynamic Scopes are used to save your inventory queries (about Identities/Accounts, Groups or Assets - or any combination) in order to reuse it in the future. The saved queries are recalculated daily so you get up-to-date visibility to your scopes. Using Dynamic Scope you can focus on what matters the most and track its progress over time.

Use cases: create detection rules, build and schedule reports, build custom dashboards.

Because platform scopes are continually updated, they are called ***Dynamic Scopes***.

System Scopes

The platform comes with a built-in System Scope, which includes account and group definitions that apply system-wide in all inventories, dashboards, and detection rules. You can customize System Scope definitions to better suit

the needs of your organization, but because System Scope definitions impact the entire platform, you must do so carefully. You can also revert your System Scope definitions back to the platform defaults at any time. The scopes are recalculated daily to provide up-to-date insights.

To view System Scope:

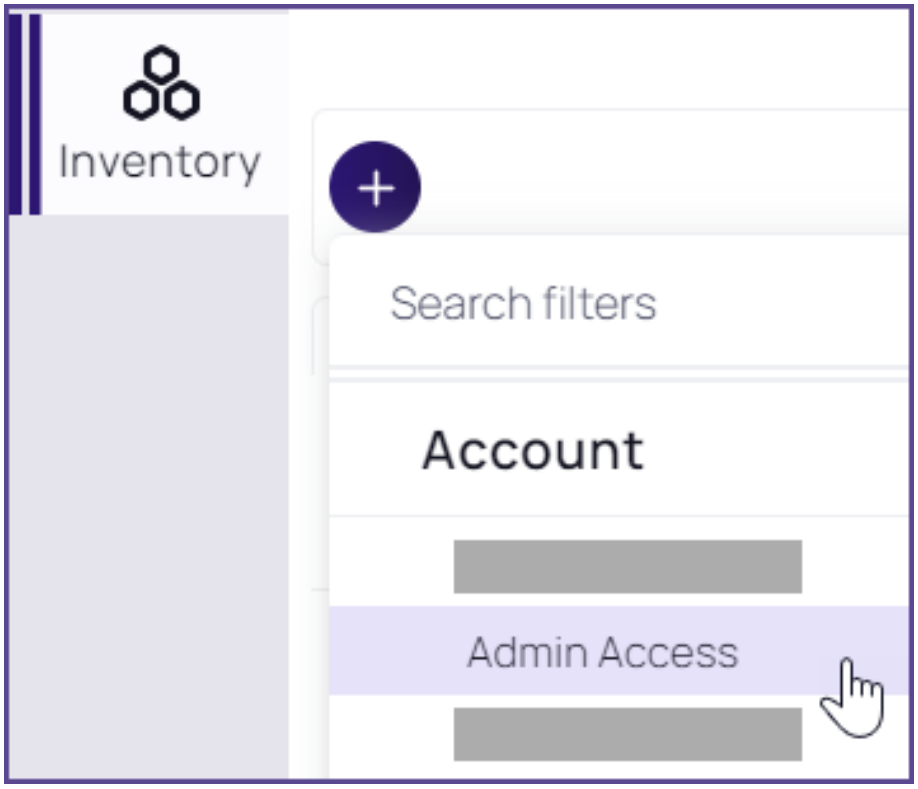
1. Choose **Inventory** > **Dynamic Scope** from the main menu.
2. Click the **System Scopes** tab.

The System Scopes page displays a table showing the accounts and groups—and the numbers of each—that match the defined system scope. For each account and group, the table displays its name, type, and status information. The table also indicates whether the System Scope definitions have been modified from the default settings. By default, the definitions are sorted by date of creation, in descending order.

Default System Scope

The built-in, default custom scope is described below.

- **Admin accounts**: which accounts are considered “admin.” To find admin accounts, you can use the **Account: Admin Access** inventory filter. For example:



- **Compliant Admin Accounts:** which accounts are considered “compliant admin.” “Compliant admin” accounts are shown in the Privileged Accounts dashboard. For example, if all admins in the organization must have an email like {full_name}_adm@company.com, define the query to find all admins with this email. The privileged accounts dashboard displays the number of non-compliant accounts according to this definition.

- **External Accounts:** which accounts are considered “external.” To find external accounts, you can use the Account: Is External inventory filter.
- **Admin Groups**: which groups are considered “admin.” To find groups that grant admin access to their members, you can use the **Group: Admin Access** inventory filter.
- **Privileged Groups**: which groups have privileged access. To find groups that grant privileged access to their members, you can use the Groups: Privileged Access inventory filter.
- **Privileged Accounts**: which accounts have privileged access. To find users with privileged access, you can use the Account: Privileged Access inventory filter.

Filter and sort the Scope table

To change the data displayed in the table, use the filters above the table. The selections you make are shown in the filter bar.

To search for a dynamic scope by name, type text in the search field to the top-right of the table.

From the Dynamic Scopes tab, you can edit, duplicate, delete, and calculate an existing dynamic scope. See "Configure the System Scope" below.

You can also create detection rules based on an existing scope. See "Create a Detection Rule from a Custom Scope" on page 534.

Insight into selected table data

The Type column shows which inventory the dynamic scope was created from.

- The Status column shows the following values:
  - Calculating
  - Exceed results – results are too large, re-run the scope 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 dynamic scope. To see the actual results, click the number in this column.

To see details about a scope, click the scope row in the table. A window showing details about the scope will open, including the query that created the scope, a description (if one was entered when the scope was created) and the last sync date.

The trend line detects rapid changes and shows how your scope changes over time, such as privilege creep or new admins, or shadow admins.

Configure the System Scope

From the System Scopes tab, you can:

- **Edit a scope**: Edit a system scope to customize the values according to your organization's needs.
- **Duplicate a scope**: Duplicate a scope 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 scope.
- **Reset a scope to default values**: Set an edited scope back to the system default.
- **Calculate scope results**: Instead of waiting for the next scheduled recalculation, you can initiate an immediate calculation of the matched accounts and groups.
- **Create a new detection rule based on a scope**: Create a detection rule based on the system scope.

Edit a scope

You can edit a system scope to customize the values according to your organization's needs.

1. Hover over a system scope.
2. From its **More** menu, click **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 Calculate a system scope .

Duplicate a scope

You can duplicate a scope 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 original scope.

1. Hover over a system scope
2. From its **More** menu, click **Duplicate**.
3. Edit the filter values and click **Save**.

The System Scopes tab shows only those scopes defined by the system. Duplicated scopes are displayed in the Custom Scopes tab.

Reset a scope to default values

You can set an edited scope back to the system default.

1. Hover over a system scope whose value in the Default column is Edited.
2. From its **More** menu, click **Reset**.

The scope value returns to the default definition, and in the Default column, the value returns to Default.

Calculate scope results

When a scope 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 (may take some time), or you can calculate scope results immediately this way:

1. Hover over a system scope.
2. From its **More** menu, click **Calculate**.

The calculation is initiated immediately. Results will be shown as soon as they are ready.

Custom Scopes

On the Custom Scopes tab, you can run a custom query on platform inventories. The query result is known as a Custom Scope, which you save and re-use. See "Save a custom scope" below. The scopes are recalculated daily to offer up-to-date insights. You can also use Custom Scopes to build custom dashboards, schedule reports, track progress over time, and create new detection rules. See "Create a Detection Rule from a Custom Scope" below.

Save a custom scope

1. Filter an inventory table.
2. Click **Save**.
3. In the Dynamic Scope Creation dialog, enter a name.
4. (Optional) Enter a description.
5. Click **Save**.

The saved custom scope is displayed in Inventory > Dynamic Scope.

Note: Saving a custom scope may take some time.

Create a Detection Rule from a Custom Scope

You can create a custom detection rule based on the filter criteria of a Dynamic Scope.

This feature is not available for dynamic scopes created from the Computers inventory.

To create a detection rule from a dynamic scope:

1. From the Scope page, click the **More** menu at the far right of the desired scope, then choose **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" on page 546.

Access Explorer

The Access Explorer is a visual display of the relationships between identities, assets, membership policies, and access policies. The Access Explorer displays membership or access policies based on the filter and source selected.

You can use the Access Explorer to find out the following:

- how an identity gains access to an asset
- which identities have access to an asset

- when access or membership was granted

Each rectangular block in the Explorer contains an icon (that represents the entity type: Asset/Identity/Account/Group) or logo (that represents an application), as well as a name, and a type.

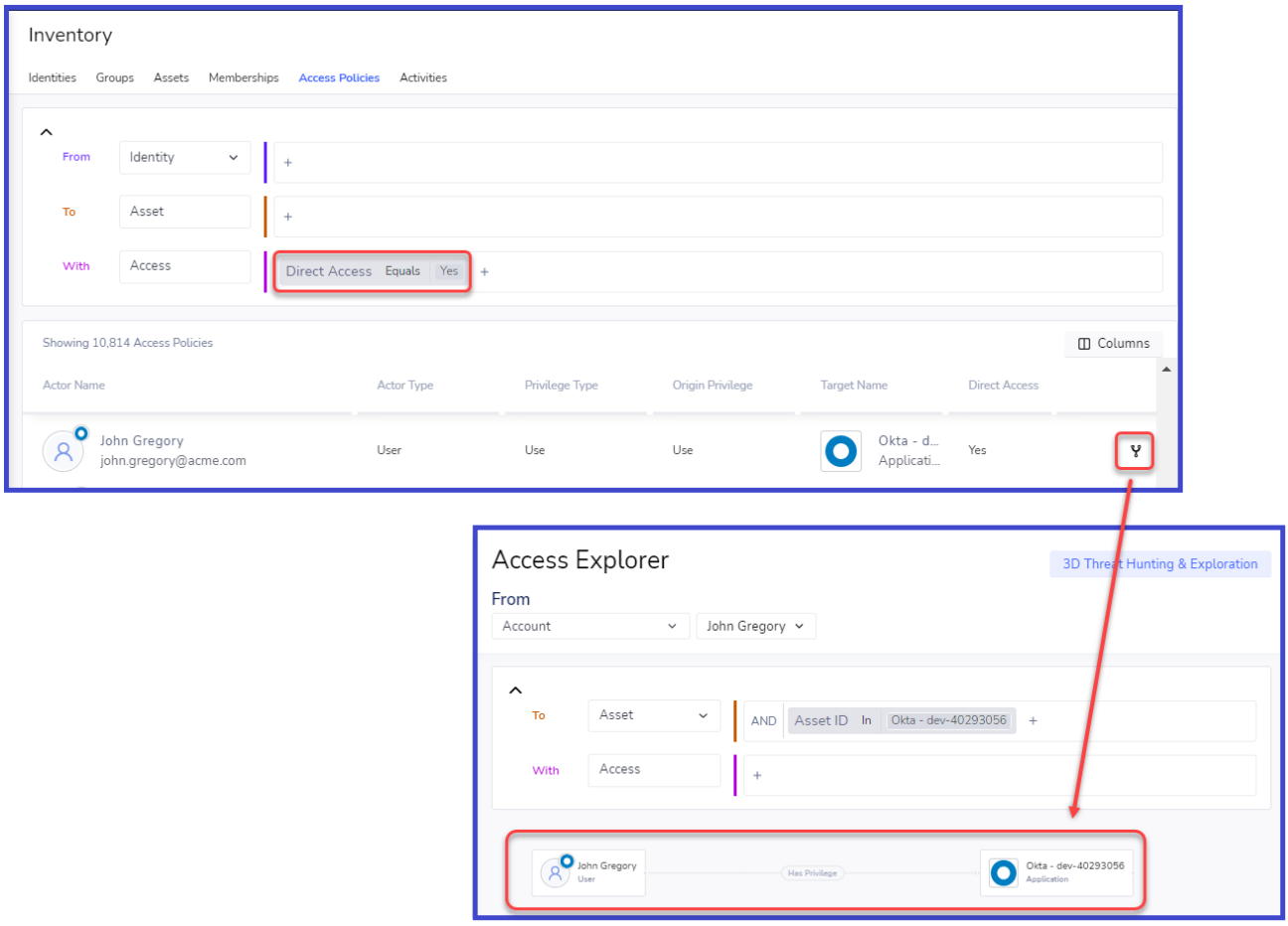
Direct vs. Indirect Access

Users can have direct or indirect access:

- **Direct access** - the actor (user, for example) has been assigned permission to an asset directly. For example, a user has read access to a file.
- **Indirect access** - the user has permission because they belong to a group or a role that enables access.

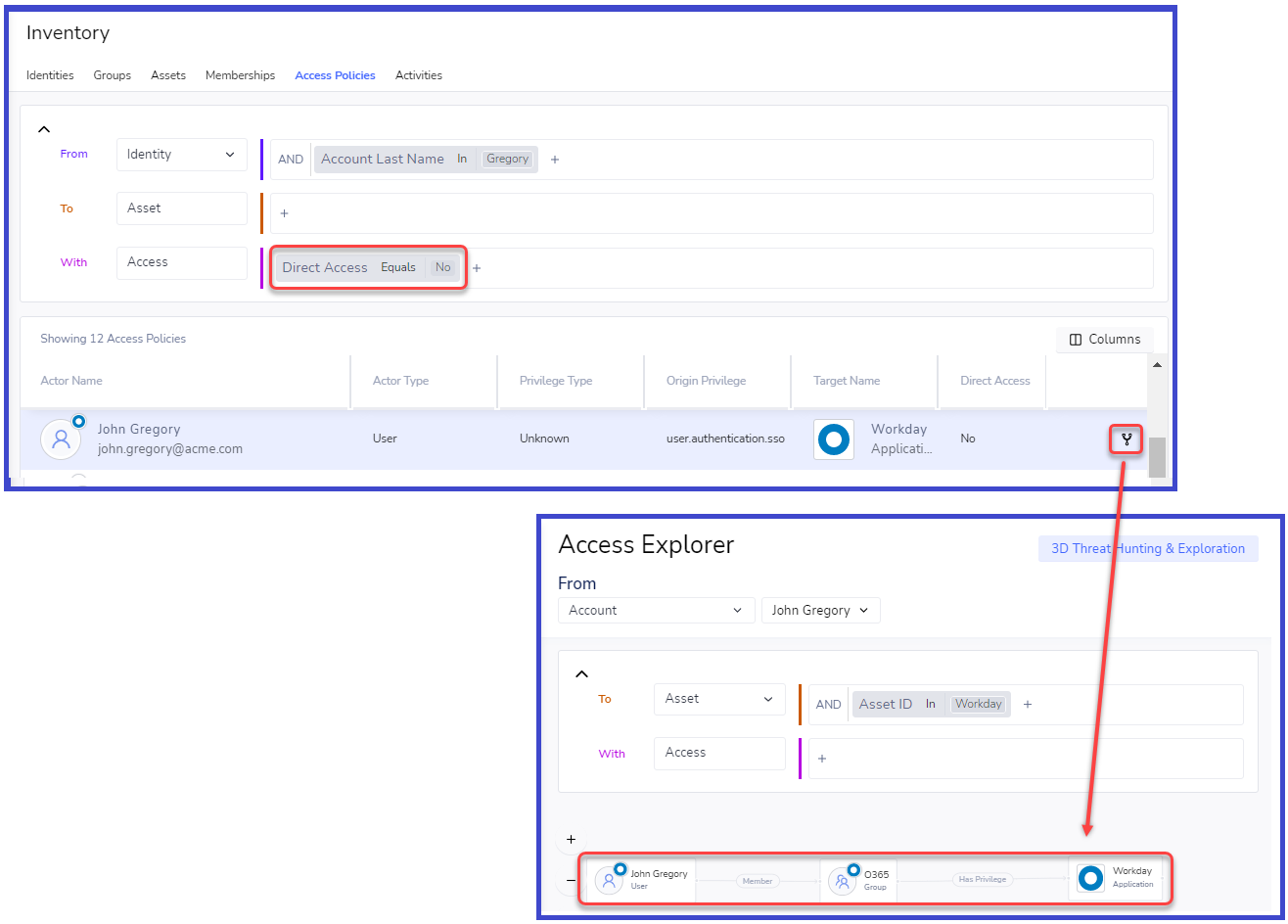
The following example shows how this is displayed in the Platform:

Direct Access Example



When you click the Access Explorer link, the Access Explorer shows that John Gregory has direct privileges to Okta.

Indirect Access Example



When you click the **Access Explorer** link, the Access Explorer shows that John Gregory is a member of the O365 group, and that the group has privileges to Okta.

In the Memberships and Access Privileges inventories, if you remove the Direct Access = Yes (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 dynamic scope (which will calculate while you are working elsewhere).

To use the Access Explorer:

1. In the **From** fields, select a source type (Identity, Account, Asset, or Group) and then the entity itself, such as a user or an asset. (If the Access Explorer was opened through one of the inventory views, the From source will already be chosen.)
2. In the **Target** field, select an option. The options will differ based on the From selection. The filters available are the same as those in the inventory in the From selection. The full list of filters is described in Inventory Filter Properties.
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

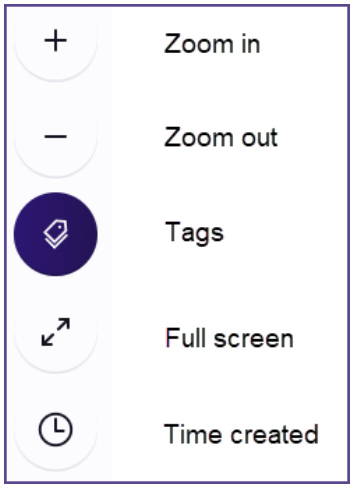
To save space in the Access Explorer graph, the platform automatically groups similar entities (assets, accounts, identities, or groups) when their privileges and applications are the same.

When looking at a group, Users and Identities are consolidated.

You can double-click on a grouping to display its contents.

Controls

In the bottom left corner of the Access Explorer graph there is a control menu:



You can use the Time created feature to see which accesses were created during a specific time. Click the clock and select a period.

Focusing on an object

Double-clicking on 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 it and move 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 informationabout the entity. In the Access Explorer graph, you can get information about each entity by hovering over it.

Note: Click on 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, enabling you to receive the most relevant information directly to your inbox.

You can define reports based on the following:

- **Dynamic scope queries**: the result of the dynamic scope query
- **Incidents**: all changes in incidents in the last 30 days

You schedule reports from the Reports page. To display the Reports page, choose **Insights** > **General Reports** from the main menu. The Reports page shows the reports that are currently scheduled. When you hover over a report line, you can delete, edit, or immediately download the report.

To create a scheduled, recurring report:

1. Click **Schedule a Report**.
2. Enter a name for the report.
3. Select the type of report to generate.
4. Select the frequency.
5. Enter the email addresses to receive the report.
6. Click **Create**.

The report will be sent according to the configuration you set.

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. This section contains the two subsections listed here:

- "Apps Overview" on the next page enables you to monitor the health of all connected user applications, both out-of-the-box and custom.
- "Checks " on page 540 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.

Onboarding Process

The onboarding process involves a straightforward approach without the need for additional permissions. Start by updating check severities if necessary and disabling irrelevant checks.

To effectively engage with the posture page, begin by exploring the Application 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.

Best Practices

Our recommendation is to have a posture score of at least 90% for each application.

We recommend solving all high severity checks within a week, medium severity checks within two weeks, and low severity checks within a month.

Regularly monitor your connected applications' posture pages and posture scores to identify configuration drifts and degraded checks. We recommend to review once a week to detect any misconfigurations right away.

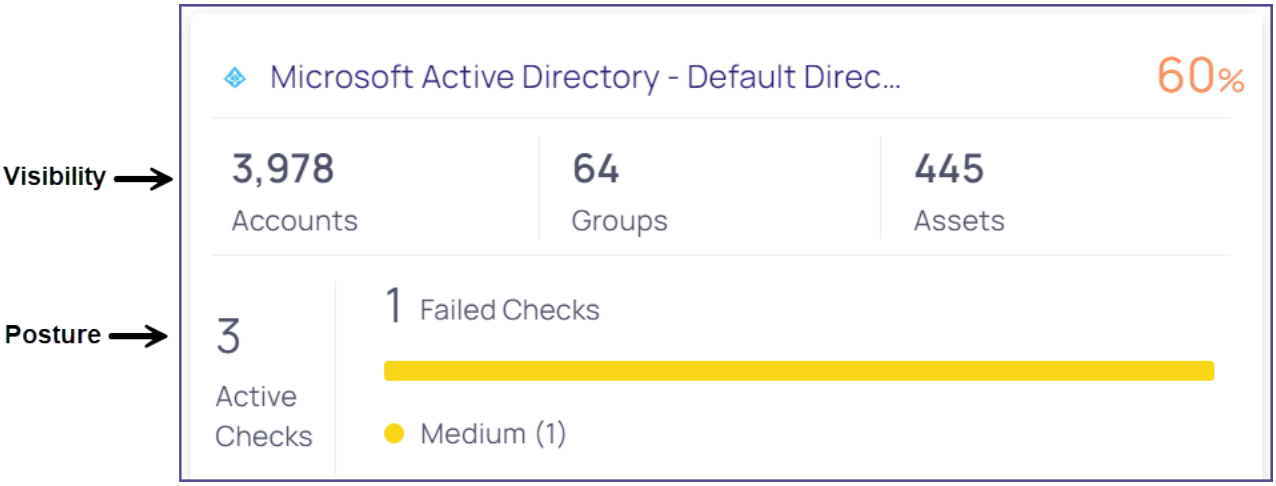
Engage your app owners in reviewing and addressing the identified misconfigurations.

Apps Overview

The Apps Overview page enables you to monitor the health of all connected user applications, both out-of-the-box and custom. The Platform assigns an identity posture score to every application to help you understand the app’s state of compliance with best-practice configuration settings. For more information, see Checks. From the Apps Overview page, you can use this score to easily find those applications that are most vulnerable, and then drill down to see exactly which issues need to be managed.

To display the Apps Overview page, choose **Identity Posture** > **Apps Overview** from the main menu.

Every app is represented by a tile.



The app tiles are sorted by posture score (ascending), from 0% (greatest risk) to 100% (least risk). The app with the lowest posture score, that is, the greatest risk, is displayed first. You can filter the page to show one app type at a time.

The app is represented by two sections:

- **Visibility**: the number of accounts, groups, and assets
- **Posture**: the number of checks performed and failed, and the severities of the failed checks. For more information, see "Checks " below.

When you click any field, you are shown 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.

Checks

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.

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.

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 involves a straightforward approach without the need for additional permissions. Start by updating check severities if necessary and disabling irrelevant checks.

To effectively engage with the posture page, begin by exploring the Application 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.

Best Practices

- Our recommendation is to have a posture score of at least 90% for each application
- We recommend solving all high severity checks within a week, medium severity checks within two weeks, and low severity checks within a month.
- Regularly monitor your connected applications' posture pages and posture scores to identify configuration drifts and degraded checks. We recommend to review once a week to detect any misconfigurations right away.
- Engage your app owners in reviewing and addressing the identified misconfigurations.

To see the Checks page, choose **Identity Posture** > **Checks** from the main menu.

The Checks page shows these parts:

- **Overview**: shows the companywide posture-related data
- **Table**: shows data specific to each check

Each row in the table represents a different check the platform runs. These checks are based on instances of applications that are integrated with the platform.

By default, the page is sorted by descending check severity. You can change the sort order by clicking a column heading.

The checks are divided into these categories to streamline management:

- **Authentication**: mechanisms used to verify the identity of users, systems, or processes
- **Privileged access**: management of access rights for 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

In addition to basic information about the check, the table shows the compliance frameworks relevant to each check, and how many entities failed the check ("affected entities").

The Checks side panel

The Checks side panel displays more details about the check and affected entities, which you can explore to remediate the issues.

To open the side panel, click a row in the table.

The Checks side panel shows more information about the check, including the security motivation for remediating the failed entities. You can also do the following:

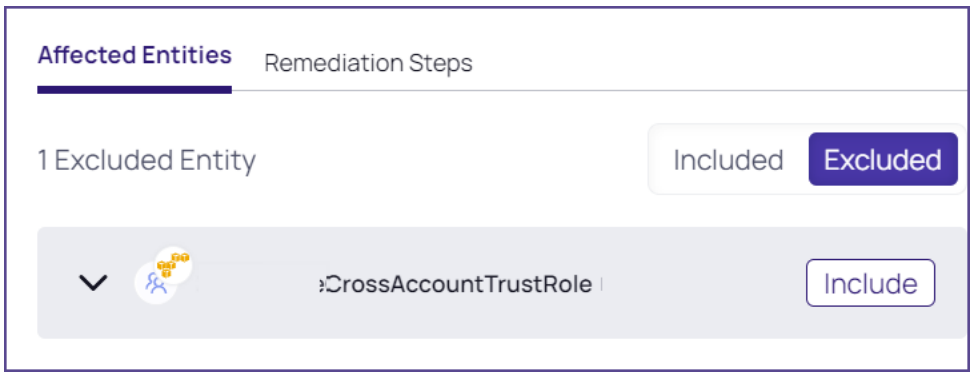
- Disable the check so it no longer runs. Some organizations are unable to follow the best-practice recommendations and they are willing to accept the risk of a misconfiguration. At the same time, they don't want their overall posture score to decrease. Disabling a check will affect the identity posture score.
- Change the severity of the check. From the Affected Entities tab, you can view and manage the affected entities.
- See why each specific entity failed the check and get a recommendation on how to fix that.
- Exclude specific entities from being included in this check. This could change the status of the check; for example, if one excludes all the entities, the check will now pass.
- From the Remediation Steps tab, you can view remediation steps.

To disable or change the severity of a check:

1. Open a check's side panel.
2. To disable the check, click **Disable**.
3. To change the severity of the check, select a severity from the drop-down.

To see and manage affected entities:

1. Open the side panel to look for a check that is in failed status.
2. All affected entities that are included are listed in the Affected Entities tab.
3. To see more information about why a specific entity failed and how to fix it, click the drop-down next to the entity name.
4. To exclude a specific entity from this check, click **Exclude** on that row.
5. Excluded entities are moved to the Excluded list:



6. To include an excluded entity, click **Include**.
7. To see general remediation steps for this check, click Remediation Steps.

Shadow Admins

Our Shadow Admin engine discovers “Shadow Admin” 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 user (identity) who can perform one of more of the following actions in one of the policies attached to it:

Actions

Action	Enables a user to...
CreateAccessKey	Create an access key for another IAM user.
CreateLoginProfile	Create another 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 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 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	Enables a user/attacker to elevate their privileges to become admins.
Microsoft.Authorization/roleDefinitions/write	Enables an attacker to update roles and escalate to administrative privileges.
Microsoft.Authorization/roleAssignments/write	Enables the user to assign other users to roles, meaning a user entitled to this role can make other admins.
microsoft.directory/users/password/update	Enables the user to reset another user's password, which can help them gain control over accounts.
microsoft.directory/users/authenticationMethods/delete	Enables removal of a user authentication method like MFA, helping an attacker to steal an account.
Microsoft.Authorization/*/Write	Enables the user to assign any role to an application and elevate its privileges.

Azure permission(s)	Description
microsoft.directory/servicePrincipals/policies/update	Enables the user to update the role assigned to a service principle, which can lead to escalated privileges.
microsoft.directory/servicePrincipals/permissions/update	
microsoft.directory/servicePrincipals/enable	Enables the user to 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	Enables the user to 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.

Azure permission(s)	Description
microsoft.directory/users/create	Enables the user to create new local users in active directory/Azure.
microsoft.directory/users/password/update	
Microsoft.Authorization/classicAdministrators/write	Enables the user to add other users as administrators.

Threat Center

Leveraging the Threat Center empowers you to execute detection rules, swiftly identifying these actions and responding promptly to mitigate each issue. Within the Threat Center, you'll encounter two primary functionalities:

"Detection Rules" below: This section presents a comprehensive catalog of both enabled and disabled rules applicable to your applications, streamlining the process of rule application and management.

"Incidents" on page 551: Incidents represent the outcomes of detection rules, offering actionable insights into detected threats. These findings, accessible within the product or via external tools, furnish detailed explanations of incidents, along with contextual data crucial for comprehending the nature of each issue.

Detection Rules

A detection rule is a set of security conditions you configure, so that when those conditions are met, the rule triggers an incident for an administrator to examine. For example, the Admin Discovered detection rule generates an incident whenever a new “admin” user is discovered. The detection rule engine runs autonomously, checking detection rules whenever a new integration is enabled, and periodically thereafter.

To see the Detection Rules page and its table, click **Threat Center** > **Detection Rules** from the main menu. By default, the Detection Rules table displays enabled detection rules from the Threat category. These are sorted by the number of incidents, in descending order.

To see more details about a detection rule, click its name and examine the side panel that is displayed.

To see the list of incidents the detection rule generated, click the number in the Incidents column, or click the **More** menu and choose **View Incidents**. For more information, see "Incidents" on page 551.

The Detection Rules Table

The Detection Rules page displays a table with the following information next to the name of each detection rule:

Column	Description	Example values
Apps	The applications that the detection rule tracks	AWS, Okta, GCP, GitHub and more

Column	Description	Example values
Severity	Severity of the detection rule	Critical, High, Medium, Low
Incidents	The number of incidents that this detection rule triggered. Closed or resolved incidents are not shown.	Number
Categories	The categories to which the detection rule belongs	Threats, Privileged Access, Stale Access, Key Management, Security Baseline, Authentication
MITRE	Related MITRE ATT&CK tactics	For example: Credential access, Initial access, Defense evasion
Channels	The enabled communication method	Email
Automated Response	Automated response is enabled (for at least one application)	True or False
Status	The detection rule status	Enabled: Incidents are created. Notifications will be sent if they were configured for the detection rule. Disabled: Detection rule is not active, and incidents are not created.
Compliance (hidden until selected)	Compliance frameworks that are relevant to the detection rule	List of relevant compliance frameworks
Owner (hidden until selected)	Displays who created this detection rule	Delinea (created by the system) [AS1] [AS2] or Other (created by user)

Filter, search, and sort the Detection Rules table

To change which checks are displayed, you can filter and sort the table's displayed data with the filters above the table. When you filter, the selections you make are shown in the filter bar. To search for a detection rule by name, type text into the search field.

By default, the table is sorted by incident count, in descending order. To sort the table differently, click a column heading to sort by. If needed, click it again to reverse the sort order.

Configure detection rules

You can do the following configuration activities to an existing detection rule:

- Enable or disable
- Edit or duplicate
- Delete

Enable or disable a detection rule

You can enable or disable a detection rule. The current status is shown in the Status column of the table. To enable or disable a detection rule, select Enabled or Disabled in the Status column. You can also do this from the detection rule side panel when editing a detection rule.

Edit or duplicate a detection rule

You can edit any existing detection rule to customize it to your needs, including system-created detection rules and rules you created. You can also duplicate an existing detection rule, for example, to create a new detection rule that is similar to an existing one. Duplicating a detection rule duplicates its logic, but not the configuration settings (like filter scopes, channels, severity, etc.). When you duplicate an existing detection rule, you will configure it and give it a unique name.

Both editing and duplicating are done in the detection rule side panel.

In addition to changing the detection rule properties (like name, status, severity) you can configure these properties:

- **Definition**: In some detection rules, this field has options to configure.
- **Filter Scopes**: Limit which entities should be detected.
- **Automated Response**: Enable or disable automated response options, depending on the options enabled in the integration and on the permissions the user granted.
- **Channels**: Enable or disable triggered notifications. To enable notifications, toggle Communication on, then:
  - **Email**: Type an address.

Global notifications will affect all enabled detection rules.

To edit a detection rule:

1. Click in the detection rule row. The detection rule side panel is displayed.
2. Configure the detection rule in the side panel.
3. When finished, click **Save Changes**.

To duplicate a detection rule:

1. Click the **More** menu at the end of a detection rule row.
2. Choose **Duplicate**.
3. Enter a name for the duplicated detection rule
4. Click **Duplicate**. The detection rule side panel is displayed.
5. Configure the detection rule in the side panel.
6. When finished, click **Save Changes**.

Delete a detection rule

You can't delete a system-created detection rule, but you can delete a user-created detection rule (one you created by duplication or from a dynamic scope).

To delete a detection rule:

1. From the Detection Rules table, click the **More** menu at the end of a detection rule row.
2. Choose **Delete**. You can also do this from the detection rule side panel when editing a detection rule. If this option is not displayed, you cannot delete the detection rule.

You can create a detection rule from a custom scope. For more information, see "Create a Detection Rule from a Custom Scope" on page 534.

Custom Polices

Custom policies empower users to identify deviations from the desired configuration, thereby enhancing overall security posture and helping to detect drift.

1. Defining Custom Scopes:

You can use custom queries to specify sensitive scopes inside your infrastructure, such as allowed permissions, resource configurations, or access policies.

2. Periodic Reporting:

Schedule reports on a weekly or daily basis, providing insights into any changes or deviations occurring within the defined scopes.

3. Real-Time Detection Rules:

Detection rules trigger real-time incidents upon detecting a drift from the defined scopes. These rules are instrumental in identifying unauthorized changes or configurations within the system. By leveraging detection rules, you can ensure timely responses to security incidents.

4. Built-In Remediation:

Our platform offers built-in remediation actions to address detected drifts, like disabling an account, adding to a group and more, for more details review the full topic.

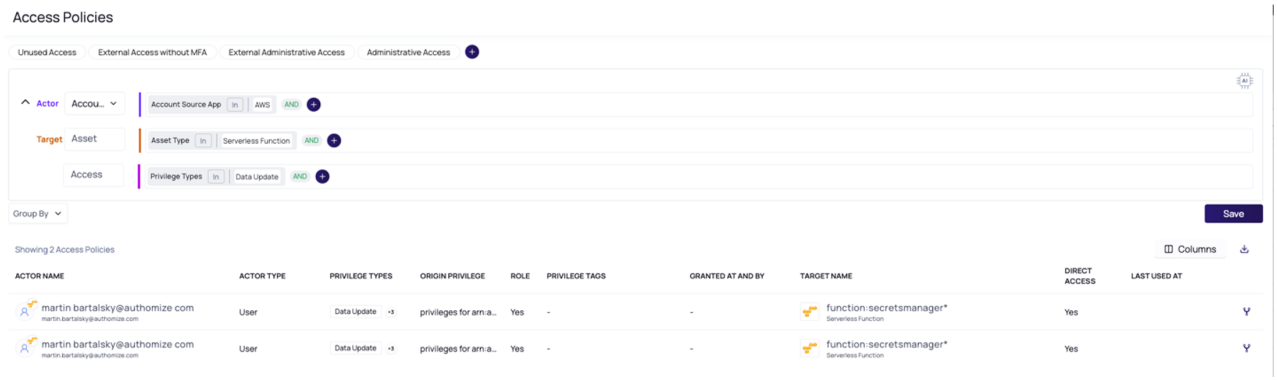
Example Scenario:

To illustrate the practical application of drift detection, let's consider the following scenario of detecting Unauthorized Access to Sensitive Data:

Objective: Identify when any local user has a data update privilege on lambda functions.

How would we achieve that?

1. **Define an Access Policy Query**: Specify a query to identify local AWS users with data update privilege on Lambda functions.



2. **Save the Query as a Dynamic Scope**: Once the access policy query is defined, save it as a scope within the platform. This scope will serve as the reference for detecting drifts in access permissions.
3. **Create a Detection Rule**: Configure a detection rule to monitor deviations from the defined scope. In this scenario, the detection rule should trigger an incident whenever a local AWS user gains permission to update a lambda function.
4. **Monitor and Respond**: Regularly monitor the drift detection incidents generated by the platform. Upon receiving an incident indicating unauthorized access, take appropriate remediation actions, such as revoking access or blocking accounts.

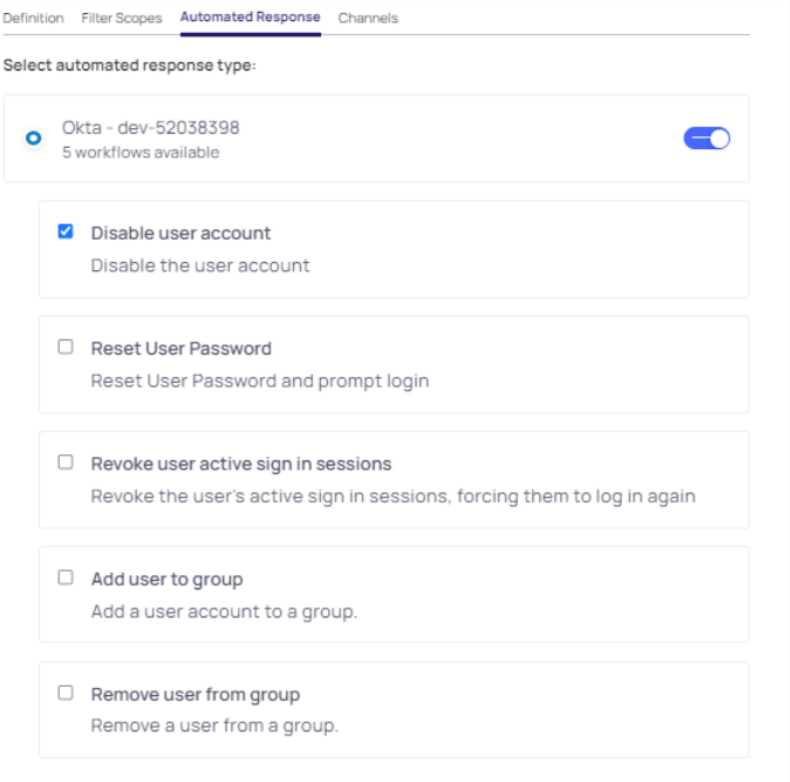
Custom detection rules is a fundamental aspect of our platform, empowering users to maintain the integrity and security of their systems and detecting drift. By leveraging custom scopes, real-time detection rules, and automated remediation capabilities, users can effectively identify and respond to unauthorized changes, thereby enhancing overall security posture.

Automated Response

There are multiple ways to apply automated response to stop threats: by enabling automated remediations, by suspending users with stale access, or by syncing with your own tools.

- Automated response: This is possible with any supported IDP, enabling you to apply automated response by setting up the response workflow with the following supported actions:
  - Suspend a user
  - Reset user password
  - Log out from all active session and trigger and MFA
  - Add to group/coronational access group to elevate additional security requirements
- Leverage the APIs or webhooks by automatically trigger and even to sync with your own existing tools such as ITSM, SIEM, SOAR and workflow engines
- Automated response via email or Slack that can be integrated to your own internal workflow and trigger an automated response

Automated response workflow example in Okta:



Incidents

To view incidents on the platform click **Threat Center** then choose **Incidents**. The Incidents page displays information about all the security or compliance events that require attention. Incidents are found by the platform, which continuously monitors your organization's assets, apps, and identities for breaches.

Note: A detection rule is a set of conditions that, when breached, generate an incident. See "Detection Rules" on page 546.

Note: Incidents are only generated from applications that are integrated with the Platform.

The Incidents page

The incidents page can display a list of incidents and a detailed view of a single incident (Single Incident Pane).

At the upper left is a number displaying the total number of filtered incidents (when filtered) and all the incidents when unfiltered. The filters appear just above the Single Incidents pane. You can use as many filters as needed by adding them one-by-one with the + button.

The Incidents list shows all the incidents when unfiltered, or just the incidents that were filtered. Each entry in the list contains several elements:

- the name of the incident
- the date the incident was reported
- a short description of the incident

- the application that is affected by the incident
- checkbox (for assigning or closing the incident)

When you click the checkbox, two options open at the bottom of the list:

- Assign (assign the issue to another platform user in your organization to review)
- Close (close the incident)

You can sort the list of incidents by clicking and selecting one of the sort options: **Newest** (default), **Oldest**, **Highest Severity**, **Lowest Severity**, or **Recently Updated**.

Bulk operations

You can assign or close multiple incidents at one time, either by selecting each incident, selecting grouped incidents, or selecting all the incidents at one time.

To perform an action to some incidents:

1. Select the incidents.
2. Click the action to perform.

To perform an action to a group of incidents:

- Select a group of incidents:
- In the Group By selection (above the incidents count), select a grouping (for example App, or Asset).
- Select the group incidents.
- Click the action to perform.

To perform an action to all incidents:

1. Select the box next to the total number of incidents.
2. To select all the incidents, click Select all X items.
3. Click the action to perform.

Filtering Incidents

The filters (above the Incident pane) enable you to focus on a specific set of incidents. To use a filter:

1. Click the **+** button.
2. Select a field.
3. Select the option in the field to filter.
4. Select as many filters as you need.

To remove a filter from your selections, click the small **x** near the filter, or hit the backspace key.

The number of incidents shows the number of incidents that were filtered. In some cases, the picklist will include the number of filtered incidents that exist.

Downloading Incidents

You can download incidents into a CSV file by clicking the download icon. If your list exceeds 5K entries, filter the content.

You can configure sending a CSV containing all incident changes in the last 30 days to recipients on a weekly, monthly, or quarterly basis. For more information, see "Recurring Reports" on page 538.

The Incidents Pane

The Incidents pane displays the incident selected in the Incident list (the first incident is the default). Most of the information about an incident appears in the Overview pane. The Graph pane displays the environment in which the incident occurred.

Editable Properties

You can change the severity, status, and assignee values by clicking them and selecting something else from the pick list.

Closing and Reopening Incidents

To close an incident, click **Close Incident** button at the top of the Single Incident Page. Closed incidents are marked as irrelevant or fixed by the client. Afterwards, the button changes to **Reopen Incident**, and clicking it reopens the incident. These actions are listed in the timeline.

If you click a resource or identity anywhere on the Incidents page, its Single Entity Page opens.

Timeline

The timeline pane displays all the activities related to the incident in reverse chronological order since the day the incident was found.

Graph

The graph pane shows the identity responsible for the incident in the environment where it was found.

Background Information

An entity can be identity or asset.

Risk Configuration

Understanding risk enables you to highlight the identified weaknesses and then prioritize actions according to the potential impact of a security breach.

Risk can be used:

- to prioritize the result of incidents by focusing first on the higher risk incidents
- to find the highest risk accounts or identities and then reduce the organizational risk

The Platform assesses account access scope, ongoing attacks, and inherent vulnerabilities in each account's security to provide a comprehensive understanding of risk.

Risk types

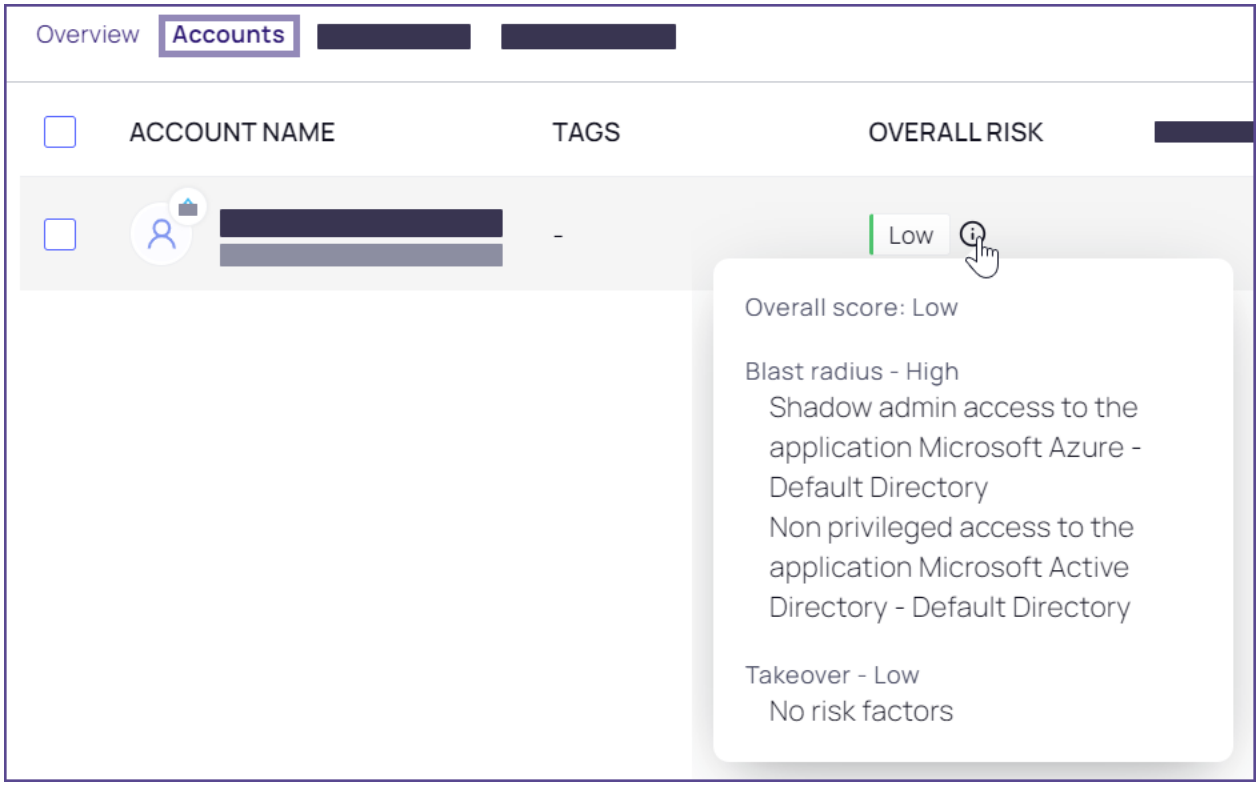
The Platform presents scores for the following types of user risk:

- **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 account or identity has. Blast radius risk incorporates account administrative access, shadow admin privileges, privileged access, and nonprivileged access.
- **Account takeover risk**: The risk of an 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).

You can see risk scores for each user on the Identities inventory tab (you may need to enable the display of these columns).

When you click a user, their 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.



Configure 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. Choose **Settings** > **Risk Configuration**. 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.
2. 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 will still be shown in the Account Takeover tab, but it will not be relevant to the score, regardless of the weight you select.)
3. Repeat for other risk factors.

Changes are saved automatically. The risk score calculation will reflect the updated weighting within 3-4 hours.

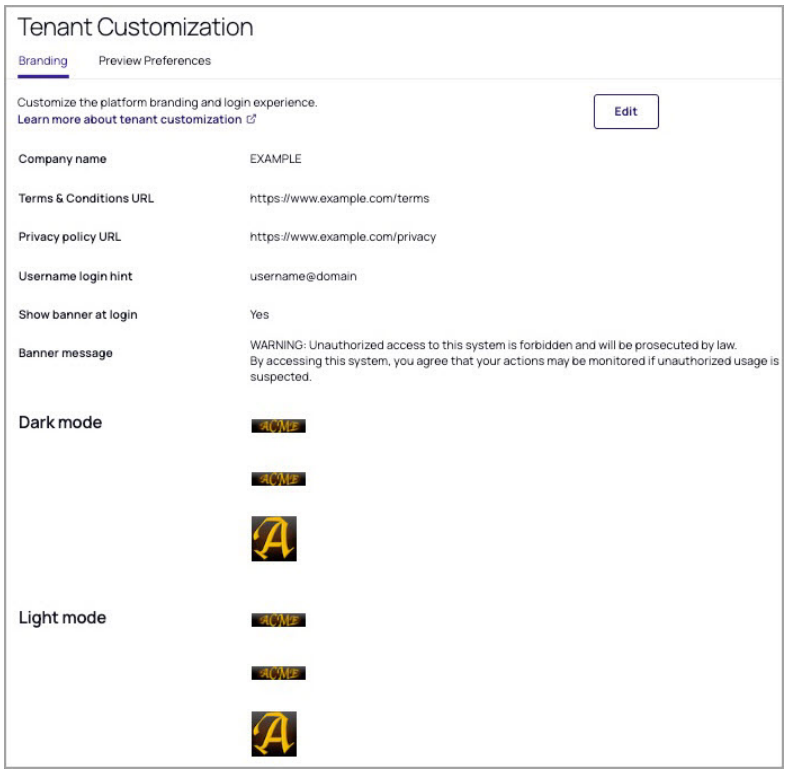
Branding

You can customize the look and feel of your Delinea Platform tenant to suit your own corporate branding and identity. This will make it clear to users that they are receiving access to the platform through your organization. These customizations will be reflected at the login prompt, and soon in the left navigation menu.

Note: If you do not see customizations applied upon first login, you may need to refresh your browser or log in again to see the changes reflected.

To customize your Delinea Platform tenant so that it looks more similar to your own company products, follow the procedure below:

1. From the left navigation menu, click **Settings**, then select **Tenant customization**. The Branding tab displays the current customization settings for your tenant instance.
2. To modify the current customization settings, click **Edit**. The page displays many fields you can use to customize your tenant.



3. Populate the tenant customization fields. The fields names are listed below, followed by guidance to help you populate each field

   Company Name: Enter your company name. It will appear below your custom logo image at the login prompt. When you populate the Company Name field, you must then also provide the URLs to your company Terms and Conditions and to your company Privacy Policy, along with your company logo image files.

   Terms & Conditions (URL): Enter the URL to your company's terms and conditions. It will then appear as a hyperlink below your custom logo at the login prompt. When you populate the Terms & Conditions field, you must then also provide your company logo image files.

   Privacy Policy (URL): Enter the URL to your company's Privacy Policy. It will then appear as a hyperlink below your custom logo at the login prompt. When you populate the Privacy Policy field, you must then also provide your company logo image files.

   Username Hint Text at Login: Provide a short sentence of hint text for login fields.

   Display banner at portal login: Enable or disable the display of a banner.

   Banner Text: Enter the text you wish to appear on your banner.

   Images for Light and Dark Mode: To successfully deploy a custom logo on the Delinea Platform, you must

upload all light mode and dark mode logo image files as specified below. These images will override the default Delinea logos presented at the login prompt and at the top of the platform's left navigation menu. When you populate the logo images, you must then also provide your company name, terms & conditions, and privacy policy links. The logo image files must meet the following specifications:

- Image file formats: JPG or PNG
- Maximum file size: 500 KB
- Maximum image dimensions:
  - Splash: 400 x 400px
  - Small banner: 200 x 50px
  - Icon: 50 x 50px

4. Click **Save** to apply your changes.

Preview Program

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

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. Click **Settings** from the left navigation menu, then click **Tenant customization.**
2. Click **Tenant**.
3. On the Preview Preferences tab, **Edit**.
4. Review the information and disclosures about the Public Preview program.
5. Select the Opt-in checkbox in the bottom left corner.
6. Click **Save**

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

Opt-out

You can choose to stop participating in the public preview at any time by simply de-selecting the Opt-in check box on shown above.

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

Feedback

The feedback received during the preview period is crucial input for further feature refinement and enhancing overall usability. You can easily submit feedback, using the feedback button near the top right corner of every platform page.

Public Preview Features

The features currently available in Public Preview will be listed in the table below. This list is subject to frequent updates. To access documentation for features currently in preview, go to the Delinea Platform documentation portal and selecting the **Public Preview** tag located in the top-right corner.

Feature	Description	Documentation

Primary Navigation

The platform's left navigation menu is designed to make all platform functions highly visible and readily accessible.

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

Primary Left Navigation Menu

Brief descriptions of all items on the new primary left navigation menu, and what you will find when you click them.

- **Home**: Set up your platform, open your applications, and browse learning resources
- **Secret Server**: See your secrets every way: 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, behavioral analytics
- **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
- **Inbox**: Notifications, system alerts, and requests at your fingertips

- **Settings**: Administrator controls for platform setup, Secret Server, connection points, directory integrations, MFA, and security

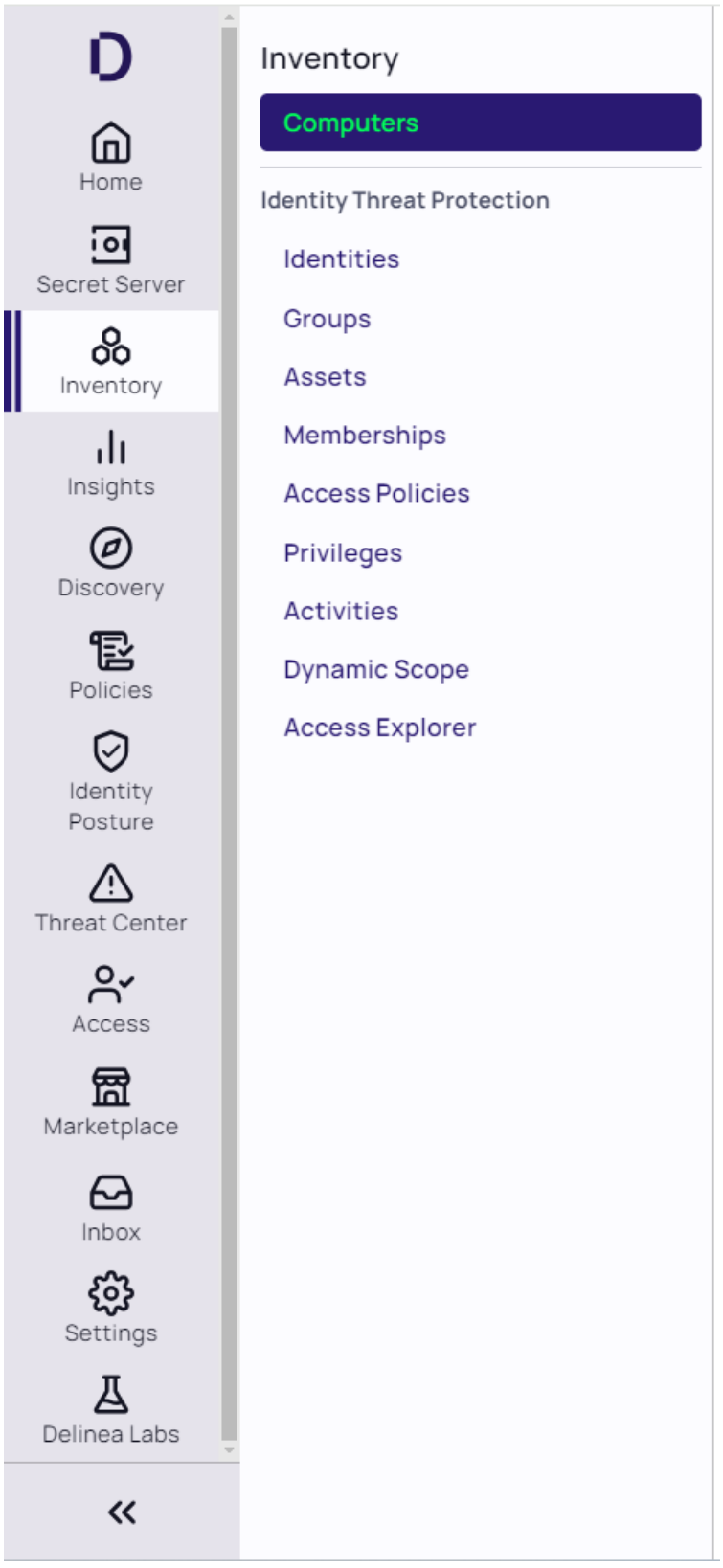
Secondary Navigation

The secondary navigation menu slides out to the right, providing a birds-eye view and immediate access to all functions relevant to the primary navigation item. This means less guessing, less searching, and fewer clicks to get where you need to be.

Hover over a menu item

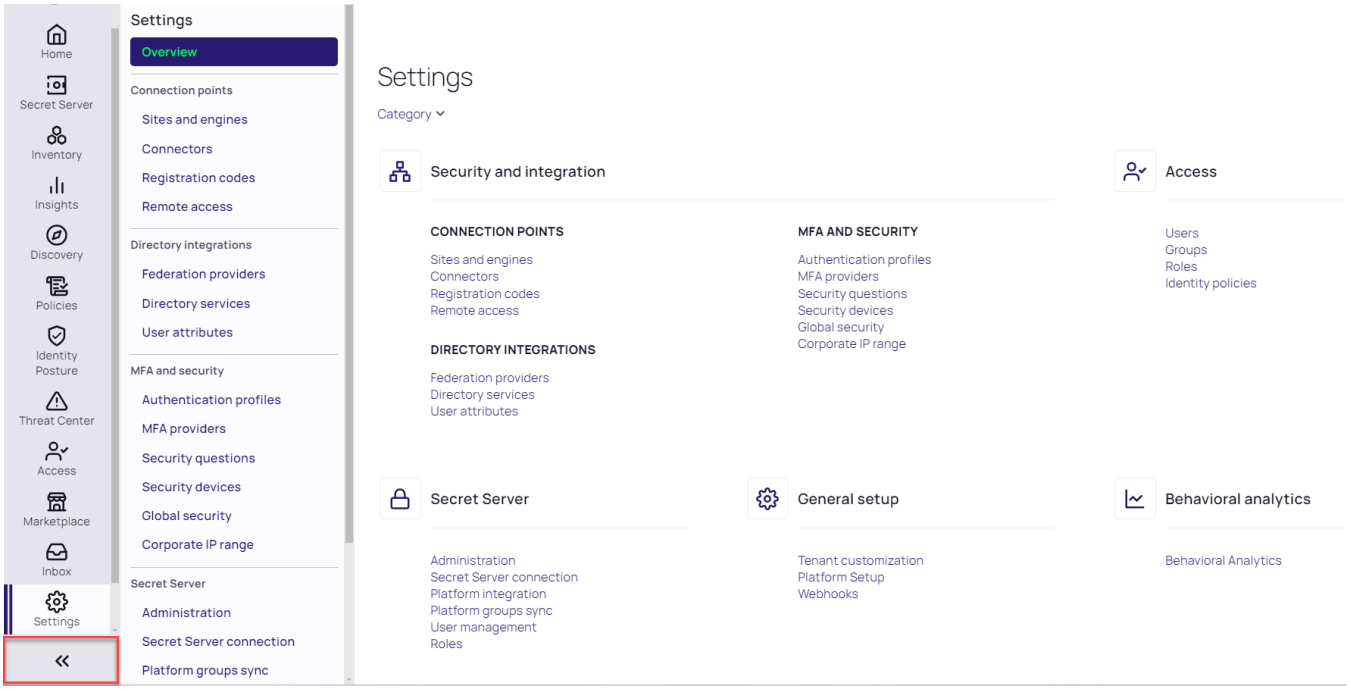
When you hover over a primary navigation menu item, the secondary navigation slides out, instantly displaying all functions related to the primary menu item. When you move your cursor away, the secondary menu slides back

behind the primary menu.



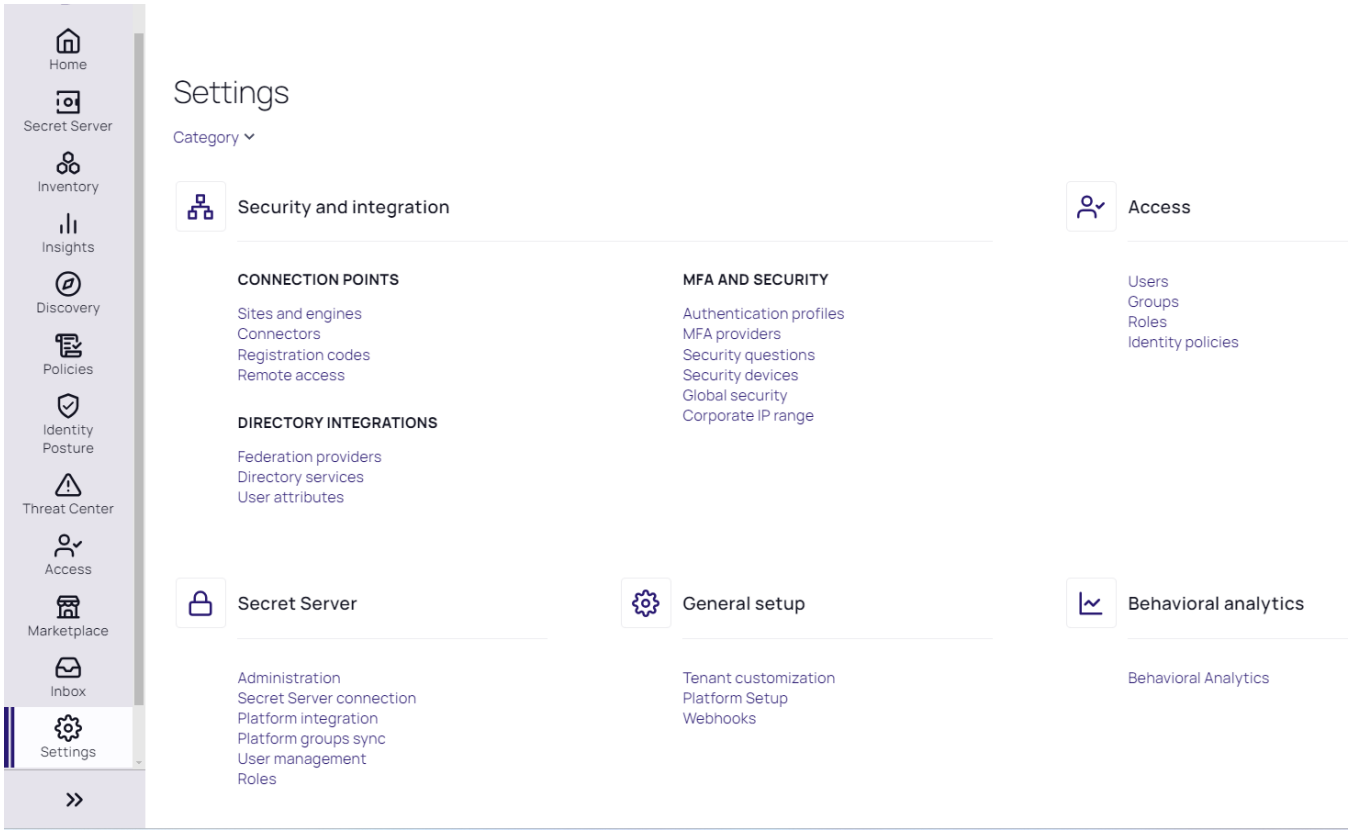
Click a menu item

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.



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



Release Notes

- Change Log
- Spring (Q2) 2024 Release
- Winter (Q1) 2024 Release
- "Fall (Q4) 2023 Release" on page 582
- "Summer (Q3) 2023 Release" on page 584
- Spring (Q2) 2023 Release
- Winter (Q1) 2023 Release

Platform Change Log

Overview

This topic contains a brief log of changes written by developers. The intent is to quickly provide information, not polished prose.

Note: The line-item numbers are for internal tracking. They provide a unique reference when talking to Delinea support.

Thursday, May 16, 2024

Improvements - 2

569469 - Marketplace - Adding Delinea Trusted badge

569164 - Marketplace - Remove Static URLs on Detail Page

Friday, May 10, 2024

Improvements - 14

566229 - Inventory - Added and enforced permission checks for Remote Applictions

564805 - Inventory - Removed duplicate API calls

566211 - Inventory - Updated the details page for Remote Applications

564725 - Inventory - Added multi-asset picker

562753 - Inventory - Added type based actions to support Remote Applications

564764 - Inventory - Remove tabs in favor of left nav

566090 - Inventory - Added additional checks and verification during tenant deprovisioning

569170 - Inventory - Removed unused event types

566209 - Inventory - Isolate translation values to their associated type

570298 - Inventory - Package updates

568799 - Inventory - Remove "Inventory" from Breadcrumb

570297 - Marketplace - Package updates

569058 - Marketplace - Set Created Date and Modified Date for new cards

569045 - Marketplace - Add Created Date / Modified Date to Marketplace API

Bug Fixes - 3

566829 - Inventory - Search Results for Assets in Global Search Not Translated

566081 - Marketplace - Fallback URL Not Working

569165 - Marketplace - Mobile QA Code Is Not Displayed

Friday, May 3, 2024

Fixes - 2

555623 - Identity - Corrected an issue where, when starting from Secret Server, using the platform login option for a federated user would not redirect back to Secret Server once login was finished.

562416 - Identity - Fix: When nesting groups, the Everybody and System Administrator groups are not listed under the Delinea directory.

Improvements - 3

553450 - Identity - Vendor PAM support for federated/AD users.

560309 - Identity - Local users Overview page has been updated to display Created on and **Last password change** fields.

563015 - Identity - new tool tips added to the user's advanced settings.

Monday, April 15, 2024

Improvements - 9

- 563115 - Inventory - Enable OS Filter Next to Search Bar
- 562751 - Inventory - Add UI configuration for action category support
- 565918 - Inventory - Removed legacy navigation resources
- 562186 - Inventory - Added single asset picker
- 562753 - Inventory - Added type based actions to support Remote Applications
- 562647 - Inventory - Various package and dependency updates
- 562750 - Inventory - Add support for dynamic inline actions
- 511135 - Inventory - Use optimistic concurrency retries in ingestion handlers
- 562176 - Inventory - Added empty state workflow for support of Remote Applications

Friday, April 12, 2024

Improvements - 3

- 563793 - Marketplace - Added AppStore URLs to v2 API
- 564801 - Marketplace - Deprecated v1 APIs

Tuesday, April 2, 2024

Improvements - 3

- 558733 - Marketplace - New Marketplace Card layout
- 562171 - Marketplace - Updates to the Marketplace SDK to support Marketing output

Bug Fixes - 1

- 562059 - Marketplace - Search term from platform search link cannot be cleared

Thursday, March 28, 2024

Bug Fixes - 3

- 559148 - Marketplace - Integrations Tab Company Name Filter Out of Order
- 561309 - Marketplace - Credential Management Category Misspelled
- 557898 - Identity - Fix: Email validator should not react on spaces at the beginning or at the end of the field

Improvements - 8

- 558855 - Marketplace - Removed unused filter fields
- 551960 - Marketplace - Include Overview Text in Marketplace Search Results
- 561741 - Marketplace - Convert front end to use v2 API calls
- 553450 - Identity - Improvement: Vendor PAM support for federated/AD users.
- 553452 - Identity - Improvement: Add audit events for Vendor PAM support
- 553643 - Identity - Improvement: Enhance admin decision-making for assigning groups to Identity policies by: Creating a dedicated step for group assignment during new identity policy creation. Introducing a “Groups” tab for managing existing policies. Updating the user experience to align with current UX patterns. Implementing a Preview Panel for at-a-glance policy review.”
- 559108 - Identity - Improvement: Add 'Require password change at next login' setting to the user add flow
- 561910 - Identity - Changing group membership on a user or group should display updated results more quickly.

Wednesday, March 27, 2024

Improvements - 3

- 560290 - Inventory - Various Improvements for deprovisioning
- 545162 - Inventory - Back end package updates
- 546140 - Inventory - Performance improvments for process large amounts of asset changes

Tuesday, March 22, 2024

Bug Fixes - 3

- 556181 - Identity - An issue that was preventing login to SSC via Platform has been resolved.
- 557397 - Identity - Fix: The identity policy descriptions were not taking effect in subsequent updates.
- 558237 - Identity - Fix: Unable to edit identity policy auth settings if policy controls are disabled.

Improvements - 2

- 549389 - Identity - Improvement: Identity updates to Angular 17
- 557280 - Identity - Improvement: UX updates to delete dialog

Wednesday, March 20, 2024

Bug Fixes - 1

- 561331 - Marketplace - Issue with Marketing output not rendering desired objects

Tuesday, March 19, 2024

Bug Fixes - 2

- 558787 - Marketplace - Vendor Drop Down Only Lists Products to Letter "O"
- 560493 - Marketplace - Duplicate Vendor in Company Name Filter

Improvements - 1

- 558854 - Marketplace - Created JSON feed for consumption by Marketing pages

New Integrations - 1

- 557435 - Marketplace - Added Monkee SAML Integration for Secret Server

Tuesday, March 12, 2024

Bug Fixes - 1

- 556193 - Marketplace - Resolved issue when the card count was not visible

Improvements - 1

- 557306 - Marketplace - Added Learn More link to associated Marketplace documentation

New Integrations - 9

- 557443 - Marketplace - Added Cisco Remote Password Changer for Secret Server
- 557444 - Marketplace - Added Oracle Remote Password Changer for Secret Server
- 557448 - Marketplace - Added UNIX Remote Password Changer for Secret Server
- 557449 - Marketplace - Added Watchguard Remote Password Changer for Secret Server
- 557451 - Marketplace - Added Office 365 Remote Password Changer for Secret Server
- 557452 - Marketplace - Added Sybase Remote Password Changer for Secret Server
- 557453 - Marketplace - Added SonicWall Local Account Remote Password Changer for Secret Server
- 557454 - Marketplace - Added VMWare Remote Password Changer for Secret Server
- 557455 - Marketplace - Added Microsoft Windows Remote Password Changer for Secret Server

Integration Updates - 1

- 557432 - Marketplace - Minor integrations metadata updates

Monday, March 11, 2024

Improvements - 3

- 547132 - Inventory - Initial onboard to audit logs
- 558105 - Inventory - Front end package updates
- 558527 - Inventory - Increased processing resources for US tenants

Friday, March 1, 2024

Improvements - 2

- 551063 - Inventory - Back end package updates
- 551325 - Inventory - Updated order of Inventory Actions

Friday, February 23, 2024

Bug Fixes - 1

- 552209 - Marketplace - Resolved issue with Company Name Filter search not returning results

New Integrations - 20

- 554064 - Marketplace - Added Splunk SOAR integration for Secret Server
- 554059 - Marketplace - Added Blue Prism integration for Secret Server
- 551691 - Marketplace - Added EntraID Remote Password Changer for Secret Server
- 551697 - Marketplace - Added Google IAM integration for Secret Server
- 551076 - Marketplace - Added RSA SecureID integration for Secret Server
- 554673 - Marketplace - Added Slack Community Integration for Secret Server
- 551699 - Marketplace - Added LDAP Credential Managment integration for Secret Server
- 551101 - Marketplace - Added Remote Password Changer for SQL Privileged Accounts in Secret Server
- 551404 - Marketplace - Added AdobeSign Community Integration for Secret Server
- 551406 - Marketplace - Added Asana Community Integration for Secret Server
- 551086 - Marketplace - Added Amazon IAM Console Community Integration for Secret Server
- 551099 - Marketplace - Added Amazon IAM Key Community Integration for Secret Server
- 551360 - Marketplace - Added Heroku Community Integration for Secret Server
- 552003 - Marketplace - Added Box Community Integration for Secret Server
- 551223 - Marketplace - Added OKTA Local User Discovery Community Integration for Secret Server
- 551224 - Marketplace - Added OKTA Remote Password Changer Community Integration for Secret Server
- 551348 - Marketplace - Added Jamf Pro Remote Passowrd Changer Community Integration for Secret Server
- 551345 - Marketplace - Added Jamf Pro Local User Discovery Community Integration for Secret Server
- 551356 - Marketplace - Added Salesforce Remote Passowrd Changer Community Integration for Secret Server
- 551225 - Marketplace - Added EntraID Local User Discovery Community Integration for Secret Server
- 551226 - Marketplace - Added EntraID Remote Passowrd Changer Community Integration for Secret Server

Integration Updates - 4

- 554090 - Marketplace - Updated Ansible integration keywords
- 551080 - Marketplace - Updated RSA SecureID for Server Suite logo
- 551376 - Marketplace - Renamed Azure to EntraID
- 549041 - Marketplace - Updated various Learn More links that were incorrect

Wednesday, February 21, 2024

Improvements - 1

- 551069 - Inventory - Updated front end packages.

Thursday, February 15, 2024

Bug Fixes - 1

- 534274 - Marketplace - Updated Marketplace card typo

Improvements - 5

- 551309 - Marketplace - Front end package updates
- 553176 - Marketplace - Back end package updates
- 549120 - Marketplace - Added "Delinea Community" badge
- 548982 - Marketplace - Updated Marketplace badges
- 550857 - Marketplace - Various API updates

Thursday, February 8, 2024

Bug Fixes - 6

- 545720 - Identity - Fix: The MFA wizard does not load initially for an invited Platform user
- 546464 - Identity - Fix: MFA redirect between non-federated users should be functional again.
- 546876 - Identity - Improvement: Rename Keep me signed in" to "Keep me logged in" inside Identity policies
- 548477 - Identity - Fixed an issue causing the incorrect IP address for the request to appear in auditing events.
- 548715 - Identity - Fix: updates to the authentication challenges description text in the authentication profile.
- 550807 - Identity - Improvement: The Next button in the Add Local User dialog is now activated once all fields are pre-filled.

Improvements - 4

- 491075 - Identity - Fix: "Keep me logged in" value was not honored and is now fixed for local and AD users. Federated user use case to be addressed separately.
- 523164 - Identity - Enhancement: Set user account to expire
- 547253 - Identity - Improvement: Ensure consistency in values reported for challenge pass-through duration across all screens in Authentication Profiles settings.

- 547897 - Identity - Improvement: Update to "Password" authentication mechanism to "Password / SSO" to support Step-up MFA for federation

Wednesday, January 24, 2024

Bug Fixes - 1

- 548508 - Marketplace - Addressed Trial Button text issue

Improvements - 11

- 520305 - Marketplace - Added Vendor Quick Filter next to Search Bar
- 548919 - Marketplace - Added Download Center tab in preparation for PCS launch
- 545612 - Marketplace - Updated badge for Ansible Integration to Delinea Certified
- 545923 - Marketplace - Added Google Authenticator for Secret Server integration
- 545926 - Marketplace - Added Omada Identity integration for Secret Server
- 545927 - Marketplace - Added Sonic Wall integration for Secret Server
- 545925 - Marketplace - Added Fortanix DSM integration for Secret Server
- 540638 - Marketplace - Added localization support
- 550021 - Marketplace - Updated description for IBM WebSphere integration
- 550019 - Marketplace - Various Learn More links were updated
- 545614 - Marketplace - Various category updates

Thursday, December 14, 2023

Bug Fixes - 4

- 529537 - Once live and the FF is enabled, will allow Federated users to follow normal MFA flow after completing their federated login. Will also allow federated users to do step-up auth similarly.
- 541441 - To enable IWA for a connector, the DNS Hostname and Iwa Certificate Subject and Alt Names should match.
- 543301 - Fix: Delinea connector 5.1.8 release to address issues with auto-update with older connectors.

Improvements - 7

- 524443 - Secret Server user licensing is now visible via Platform.
- 526986 - Enhancements: Introduce the capability to disable and enable user accounts New UX/UI refactor of the user management table and detail screen.
- 530838 - Improvement: If no registration code is present while adding a new connector, the "Copy from existing" radio button is now disabled. Additionally, the order of selections has been flipped for improved usability.
- 537757 - Improvement: Delinea connector 5.1.7 release. Improvement in reliability and extensibility.
- 538100 - Enhancement: new description field added to the authentication profiles

- 542268 - Enhancement: Now, users can directly download the connector from the primary Connector settings screen

Tuesday, November 28, 2023

Improvements - 6

- 540949 - Marketplace - Added PostgreSQL Remote Password Changer
- 539421 - Marketplace - Added Trusona Vault Passwordless Authentication integration
- 540964 - Marketplace - Added Salesforce Remote Password Changer
- 540952 - Marketplace - Added SAP Remote Password Changer
- 540986 - Marketplace - Added SQL Server Remote Password Changer integration
- 540992 - Marketplace - Added IBM Remote Password Changer

Monday, November 20, 2023

Improvements - 4

- 539422 - Marketplace - Updated TwoSense integration details
- 539425 - Marketplace - Updated Axonius integration details
- 539579 - Marketplace - Updated DevOps Secret Vault remote password changing details
- 539578 - Marketplace - Updating Oracle Remote Password Changer integration details

Tuesday, November 7, 2023

Improvements - 4

- 538311 - Marketplace - Updated RAS card description
- 539073 - Marketplace - Updated "Learn More" link for SecureLink integration
- 539102 - Marketplace - Updated CloudSuite ServiceNow description
- 538341 - Marketplace - Added DSV Remote Password Changer integration

Wednesday, November 1, 2023

Bug Fixes - 1

- 536883 - Marketplace - Addressed issue with company filter not applying

Tuesday, October 31, 2023

Bug Fixes - 5

- 524267 - Fixed an issue that sometimes caused incorrect user status to show on the user grid and user status page

- 526703 - Federated users that are part of a federation with group mappings configured will now be removed from any platform groups mapped to federation groups that they are no longer members of in their respective federation upon login.
- 527899 - Added body arguments for the SetProxyIwaHostCertificateFile API
- 530636 - User showing up in Roles as "API" has been resolved
- 534132 - Corrected an issue where the Secret Server settings tab could be visible prematurely when viewing groups in Platform.

Improvements - 4

- 523783 - Added new validation to check the IWA Hostname against certificate hostnames.
- 523784 - Improvement: fix and simplify the IWA setup process of uploading the connector host certificate
- 524443 - Secret Server user licensing is now visible via Platform.
- 530496 - Changed the connector install/registration screen wording to better reflect the optional nature of the Deleted Objects screen and rights needed by the connector. This is to help avoid customer confusion.

Wednesday, October 25, 2023

Bug Fixes - 1

- 536837 - Registration - Created new migration to approve pre-existing Registrations that are derived from Registration Codes of Automatic deployment type. Migration will also repair Registrations that are missing Service User accounts.

Improvements - 1

- 527815 - Registration - Deployed to development.

Tuesday, October 24, 2023

Bug Fixes - 3

- 530254 - Marketplace - Removed duplicate entry in Company Name filter
- 535721 - Marketplace - Updated cards with IBM Strategic Partner badge
- 536462 - Marketplace - Updated Google Identity DevOps integration title

Improvements - 8

- 534732 - Marketplace - Updated Delinea Certified tooltip text
- 535546 - Marketplace - Added Terraform Secret Management for Secret Server integration
- 536190 - Marketplace - Added AWS Discovery for Secret Server
- 536180 - Marketplace - Added Active Directory Discovery for Secret Server
- 536193 - Marketplace - Added Google Cloud Platform Discovery for Secret Server
- 536198 - Marketplace - Added Unix Discovery for Secret Server

- 536199 - Marketplace - Added VMware Discovery for Secret Server
- 536383 - Marketplace - Added Keyfactor Command for Secret Server integration

Wednesday, October 11, 2023

Bug Fixes - 1

- 531369 - Marketplace - Addressed scenario where filter selection did not return results.

Improvements - 6

- 534149 - Marketplace - Added Azure AD with SAML integration
- 534150 - Marketplace - Added Okta SAML Federation integration
- 534167 - Marketplace - Added Ping Identity SAML integration
- 534151 - Marketplace - Added Auth0 SAML integration
- 534123 - Marketplace - Added DSV Kubernetes Secret Synchronizer integration
- 534199 - Marketplace - Added Twosense SSO integration

Tuesday, October 3, 2023

Improvements - 4

- 533751 - Marketplace - Updated various download URLs
- 525229 - Marketplace - Added MremoteNG Integration
- 529255 - Marketplace - Added Jenkins Secret Server Integration
- 530825 - Marketplace - Added ArgoCD Integration

Tuesday, September 26, 2023

Bug Fixes - 2

- 523116 - Remote Access Service - Fixed an issue where UI was not handling nulls when showing error messages.
- 529523 - Remote Access Service - Fixed an issue where an error "Request Header Or Cookie Too Large" is shown when cookies size is high.

Improvements - 5

- 525076 - Remote Access Service - Added support to configure Remote Apps using the Secret Metadata fields
- 526058 - Remote Access Service - Improved performance of auto selecting the Remote Access Service site during the launch
- 526278 - Remote Access Service - Added support to not to prompt for the computer ip/dns when remote access sessions are launched from Inventory using Active directory template secrets
- 528113 - Remote Access Service - Launchers not supported for Remote Access are no longer prompted
- 530107 - Remote Access Service - Fixed intermittent session disconnects when refreshing auth tokens

Friday, September 15, 2023

Bug Fixes - 5

- 520834 - Fixed an issue that would cause users created from Federated logins to be missing their username if "userprincipalname" wasn't provided as a claim in the SAML/OIDC response assertion.
- 522396 - Fix: Receive timeout setting for Radius MFA Provider now translates seconds to milliseconds to conform to backend API.
- 523474 - Fixed an issue related to connector showing setup is incomplete message.
- 524216 - The records on the Console-Diagnostics Feature Flags page now display correctly when many flags are present and sorting is now enabled. The records on the User Management User Activity page now display correctly when many records are present.
- 524271 - Fix: Non-admin users can now delete their own passcodes.

Improvements - 8

- 517967 - External Radius MFA mechanism is now enabled by default.
- 518568 - The display name of the secret Vault is now set via the Platform. The Vault subcategories for Reporting, Inbox, and administration have been updated to reflect Secret Server.
- 519632 - Improvement: connector status and ping information is now up to date and accurate
- 520457 - Improvement: updates to the Multi-Factor Authentication Providers settings card description, instructions, and support for delete action inside the detail screen.
- 520883 - Users has a new optional federation source on their activity.
- 523784 - Improvement: fix and simplify the IWA setup process of uploading the connector host certificate

Tuesday, September 12, 2023

Improvements - 8

- 519035 - Marketplace - Vendor filter added to Applications and Integrations tab
- 520302 - Marketplace - Certification Level Badge and tooltip moved to be in-line with top of the card.
- 523541 - Marketplace - Supported Applications filter added to Applications and Integrations tab
- 523093 - Marketplace - Added Teradata integration card
- 523280 - Marketplace - Updated Rapid7 Integration card
- 523500 - Marketplace - Updated XSOAR Integration card
- 528120 - Marketplace - Updated link in Terraform Integration card
- 523169 - Marketplace - Security updates

Thursday, August 3, 2023

Improvements - 1

- 520833 - Marketplace - Enabled Global Search for Marketplace items

Friday, July 28, 2023

Bug Fixes - 6

- 484874 - Fixed switching away from the browser tab with RAS RDP session opened and coming back after few mins disconnects the session.
- 512531 - Engine update button is disabled while the upgrade is in progress.
- 518327 - Fixed incorrect icon and learn more link is shown when session is successfully exited
- 520130 - Fixed header styles for site details modal
- 520459 - Fixed error message when tunnel/session id is not found
- 520612 - Verified the bug and it's working as expected after a successful engine upgrade

Improvements - 6

- 473070 - Improve error messages on session launch when the user has no access to the Secret
- 512542 - Improved error message for unexpected error
- 513972 - Updated new UI for secret templates page
- 519657 - When enabled by feature flag, RDP sessions now have clipboard disabled if the Secret Server secret has clipboard access disabled.
- 520062 - Clipboard action on the remote desktop portal now displays an error message when clipboard access is disabled on the RDP Session.
- 510641 - Improvements to engine updater to self-update

Thursday, July 27, 2023

Improvements - 1

- 522072 - Marketplace - Integration card updates and additions

Bug Fixes 1

- 522070 - Marketplace - Minor UI bugs

Friday, July 21, 2023

Improvements - 5

- 465938 - Identity - Fix: Introducing a convenience cookie to support 'Remember and suggest last used authentication factor' policy setting
- 514666 - Identity - New Vault User Details in the Platform overview for Users tab. It requires a vault to be successfully connected and configured for the details to appear, otherwise the section does not appear.
- 517784 - Identity - Improvement: The user's Type field was renamed to Source Directory for added consistency.
- 518081 - Identity - Improvement: Updated download link for the Delinea Connector
- 519724 - Identity - Improvement: Added a preview panel for connector details

Wednesday, July 5, 2023

Improvements - 1

- 517168 - Marketplace - Updated Marketplace Overviews and badging.

Wednesday, June 28, 2023

Improvements - 1

- 504582 - Marketplace - Marketplace grid filter updated to allow robust filtering and searches.

Wednesday, June 14, 2023

Improvements - 5

- 482522 - Federation - Add an OIDC setting to send prompt=login or prompt=select_account in the login request, and a SAML setting to send ForceAuthN in the login request.These settings, if recognized by the identity provider, allow us to require users always enter their credentials on the calling identity provider rather than logging in without a prompt. Default behavior is current behavior, which is "Not Specified" for OIDC and false for SAML.
- 491152 - Marketplace - Updated Marketplace to use latest, non-breaking change, versions of Delinea components and packages.
- 491677 - Marketplace - Updated all Marketplace cards to point to point at delinea.delinea.app/doc/api.
- 504582 - Marketplace - Marketplace grid filter were updated to allow robust filtering and searches.
- 504680 - Marketplace - Marketplace 2.0 UI changes have been introduced to allow faster and easier product view and

Wednesday, June 7, 2023

Bug Fixes (2)

- 509721 - RAS - Performance improvements to address live session delay and recorded session truncation issues.
- 511559 - RAS - Fixing loader/Spinner icon was not displaying while launching the remote session.

Improvements - 4

- 486085 - RAS - Added support to launch remote access sessions using the credentials manually provided by the user.
- 507984 - RAS - Show better error message when user lacks enough RDP permissions on the target system.
- 509162 - RAS - Added support to skip Site selection dialog during the session launch if the Remote Access Site name matches with the Secret Server Site set on the Secret.
- 510812 - RAS - Added support to show Secret name in the Session Recordings.

Wednesday, May 10, 2023

Bug Fixes - 6

- 509748 - Federation UI update to ensure group mapping "remove" button is displayed and visible to the user
- 469436 - Fixed showing proxy ip/dns instead of target system ip/dns in remote access browser tab and session recording asset id.
- 504352 - Use Domain field set AD template Secrets for RDP sessions
- 504356 - Fix showing Update action on the engine when its version is higher than the released version.
- 504989 - Fix intermittent issue of Remote Access link doesn't show up on the top nav for OnPrem Secret Server configured tenant
- 506434 - Fix UI error after launching RAS session with computer IP prompt field

Improvements - 5

- 508411 - Improvement: cards are displayed in a consistent and predictable manner under Administration and User Management
- 504169 - Fix showing error message on session launch for un-expected errors
- 505177 - Updates to published RAS Public APIs documentation
- 508196 - learn more doc link is left aligned in the install engine modal
- 489501 - Open Telemetry configuration added so traces can now appear in DataDog

Monday, April 17, 2023

Bug Fixes - 8

- 486205 - Fixed UI bug where the delete role member button could be clicked multiple times causing errors
- 486208 - Fixed bug allowing add role members to be clicked multiple times
- 487562 - Fixed UI bug where the Everybody Group as displaying incorrectly
- 490746 - Fixed Javascript errors in Production
- 500780 - Fixed bug preventing provisioning of new tenants on permissions
- 501093 - Fixed bug causing out of memory exception in the Permission Service
- 502596 - Fixed bug where the delete icon was displaying for Built-In roles
- 464709 - Manage storage lifetime of SAML tokens in Federation service

Improvements -10

- 485990 - Added in-line delete icons on Role Membership for Users and Groups
- 489518 - Changed the Analytics permission name from Analytics to behavioralanalytics
- 490857 - Added a new Permission to view the Marketplace in the left navigation
- 491668 - Renamed the TenantProfile Permission name from delinea.platform/tenantprofile/admin/update to: delinea.platform/administration/tenantprofile/update
- 500287 - Performance increase for Permissions API
- 500518 - Updated the Permission Service UI to Angular 15

- 500844 - Add in-line delete icons for Roles and Permissions
- 501193 - Updated the help text on the User roles page
- 501539 - Improved performance of processing RAS audit events
- 502568 - Upgrade Remote Access Service Web App to Angular 15

Monday, April 10, 2023

Improvements - 1

- 504106 - Upgrade federation configuration web app to Angular 15

Wednesday, March 29, 2023

Bug Fixes - 3

- 484231 - Fixed filters loading for session recordings
- 500363 - Reset play button state when video context is changed
- 502683 - Fix UI issue with Audit menu loading

Improvements - 7

- 481265 - Performance Improvement to reuse AMQP channels
- 485200 - Map Secret Server event codes to the proper types
- 490299 - Standardize size of Session Recording cards
- 490739 - Add additional automated QA
- 501245 - Add universal token support
- 501675 - Fix issues with end-to-end testing

Friday, March 17, 2023

Improvements - 1

- 503998 - Increased the timeout of MFA sessions to better support email servcies that delay email delivery

Wednesday, March 15, 2023

Bug Fixes - 3

- 487587 - Remove custom metadata label that was propagating to all services' tables
- 490240 - Fix issue with search bar showing no results
- 490654 - Fix display bug for when session table is loaded with no sessions present

Improvements - 4

- 487582 - Add delete endpoint to EventMapping API; Update EventMapping API sheet indexes to names; Update Core and Mapping Single Upload Endpoints
- 489194 - Utilize common platform redis service specific to data boundaries

- 490050 - Conform date times to common Platform formatting
- 491877 - Add static build of angular 13 to deployment to allow for in-place upgrade to angular 15

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.

Remote Access Service (RAS)

- 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, RAS will use SFTP (more secure overall). If only SMB is available, RAS 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 RAS 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 RAS 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 logins, 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
  - Remote Access Service
  - 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 Remote Access Service 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.

Engine Management

- 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.

Remote Access Service (RAS)

- File transfer to and from SSH targets
- RAS engine host sizing guide
- RAS 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.

Remote Access Service (RAS)

- Introducing enhanced control for RAS 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

Marketplace & Integrations

- 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 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 (Multi 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

Remote Access Service (RAS)

- Additional logging and diagnosability to effectively identify and resolve issues
- Support for HTTPS PROXY by the RAS 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.
- Connector auto-update support: you no longer need to manually download and install 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 Remote Access Service

- 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