One Identity Safeguard for Privileged Passwords 7.4

Administration Guide

Copyright 2023 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (http://www.OneIdentity.com) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at http://www.OneIdentity.com/legal/patents.aspx.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal/trademark-information.aspx. All other trademarks are the property of their respective owners.

Legend

WARNING: A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

SPP Administration Guide
Updated - 14 September 2023, 17:05

For the most recent documents and product information, see Online product documentation.

Contents

Introduction **19**
Introduction to One Identity Safeguard for Privileged Passwords 19
Overview of the entities 21
Appliance specifications 27
System requirements and versions **31**
Web client system requirements 32
Web management console system requirements 32
Supported platforms 33
Licenses 40
Long Term Support (LTS) and Feature Releases 42
Using API and PowerShell tools **44**
Using the API 44
Customize the response using API query parameters 47
Using Safeguard PowerShell 49
Using the virtual appliance and web management console **50**
Setting up the virtual appliance 52
Virtual appliance backup and recovery 55
Support Kiosk 56
Cloud deployment considerations **60**
AWS deployment 62
Azure deployment 64
OCI deployment 66
Virtual appliance backup and recovery 68
Setting up Safeguard for Privileged Passwords for the first time **69**
Step 1: Create the Authorizer Administrator 69
Step 2: Authorizer Administrator creates administrators 70
Step 3: Appliance Administrator configures the appliance 70
Step 4: User Administrator adds users 71
Step 5: Asset Administrator adds managed systems 72
Step 6: Security Policy Administrator adds access request policies 72

Using the web client **74**
My Settings 75
Change password 76
FIDO2 keys 77
Application switcher 77
Log out 78
Search box 78
Search by attribute 79
Exporting data 80
Home page **82**
My Requests 83
Personal password vault 85
Approvals 90
Reviews 91
Favorites 92
Privileged access requests **94**
Configuring alerts 95
Email notifications 95
Password release request workflow 95
Requesting a password release 96
Taking action on a password release request 98
Approving a password release request 100
Reviewing a completed password release request 101
SSH key release request workflow 102
Requesting an SSH key release 102
Taking action on an SSH key release request 104
Approving an SSH key release request 106
Reviewing a completed SSH key release request 107
API key release request workflow 108
Requesting an API key release 108
Taking action on an API key release request 110
Approving an API key release request 112
Reviewing a completed API key release request 113
Session request workflow 113

About sessions and recordings 114
Requesting session access 114
Taking action on a session request 117
Approving a session request 119
Launching the SSH client 120
Launching an RDP session 120
Configuring and launching a Remote Desktop Application session 121
Reviewing a session request 122

Appliance Management 124

Appliance 124
Appliance Diagnostics 126
Appliance Information 127
Shutting down the appliance 128
Restarting the appliance 129
Setting the appliance name and Host DNS Suffix 129
Debug 130
Licensing settings 131
Factory Reset 133
Lights Out Management (BMC) 135
Network Diagnostics 137
ARP 138
Netstat 138
NS Lookup 138
Ping 139
Show Routes 139
Telnet 139
Throughput 140
Trace Route 140
Networking 141
Operating System Licensing 144
SSH Algorithms 144
Patch Updates 146
Power 147
Support bundle 148
Time 149

Time Zone ... 151
Backup and Retention ... 151
About backups ... 152
Archive servers ... 152
Adding an archive server ... 153
Audit Log Maintenance ... 156
Backup and Restore ... 161
Run Now ... 163
Download a backup ... 164
Upload a backup ... 165
Restore a backup ... 166
Archive backup ... 167
Backup settings ... 168
Backup protection settings ... 170
Backup Retention ... 171
Authorize VM Compatible Backups ... 172
Certificates ... 173
About Certificate Signing Requests (CSRs) ... 174
Audit Log Signing Certificate ... 175
Creating an audit log Certificate Signing Request ... 177
Installing an audit log certificate ... 178
Certificate Signing Request ... 179
Hardware Security Module Certificates ... 180
Installing a Hardware Security Module client certificate ... 183
Assigning a Hardware Security Module client certificate ... 183
Uploading a Hardware Security Module server certificate ... 183
SMTP Certificate ... 184
Creating an SMTP Certificate Signing Request ... 185
Installing an SMTP certificate ... 185
SSL/TLS Certificates ... 187
Creating an SSL/TLS Certificate Signing Request ... 188
Installing an SSL/TLS certificate ... 189
Assigning an SSL/TLS certificate to appliances ... 190
Syslog Client Certificate ... 190
Creating a syslog client Certificate Signing Request ... 192

Installing a syslog client certificate 192
Trusted CA Certificates 193
Adding a trusted certificate 194
Removing a trusted certificate 195
Cluster 195
Cluster Management 196
Unlocking a locked cluster 199
Task delegation in a cluster 200
Password distribution in a cluster 201
Managed Networks 201
Adding a managed network 204
Deleting a managed network 205
Resolving IP address 205
Offline Workflow (automatic) 205
Enable automatic Offline Workflow 207
Manually override automatic Offline Workflow 207
Session Appliances with Safeguard for Privileged Sessions link 208
Connection deletion: soft delete versus hard delete 211
Global Services 212
External Integration 217
Email 218
Enabling email notifications 219
Email Events 220
Add an email event 221
Email Templates 222
Hardware Security Module 223
SNMP 226
Configuring SNMP subscriptions 227
Verifying SNMP configuration 228
Starling 229
Join Starling 229
After joining Starling 230
Unjoin Starling 232
Syslog 232
Configuring and verifying a syslog server 234

Syslog Events ... 236
Add a syslog event subscriber ... 237
Ticket systems ... 238
ServiceNow ticketing system integration ... 239
Remedy ticketing system integration ... 240
Not integrated with ticketing system ... 241
Trusted Servers, CORS, and Redirects ... 242
Real-Time Reports ... 244
Safeguard Access ... 245
Messaging settings ... 245
Login Notification ... 246
Message of the Day ... 246
Local Login Control ... 247
OAuth 2.0 Grant Types ... 250
Local Password Rule ... 251
Modifying user password requirements ... 251
Identity and Authentication ... 254
Authentication provider combinations ... 256
Adding identity and authentication providers ... 259
Branding Customization ... 270
Appliance Management Settings ... 271

Asset Management ... 272
Account Automation ... 272
Accounts ... 273
Properties (account) ... 274
Owners tab (account) ... 278
Dependent Assets (account) ... 279
Access Request Policies (account) ... 280
Check and Change Log tab (account) ... 281
Discovered Services tab (account) ... 282
Discovered SSH Keys (account) ... 283
History tab (account) ... 285
Managing accounts ... 286
Adding an account ... 286
Adding a cloud platform account ... 288

Manually adding a tag to an account 289
Deleting an account 290
Adding users or user groups to an account 291
Checking, changing, or setting an account password 291
Viewing password archive 292
Checking, changing, or setting an SSH key 292
Viewing SSH key archive 294
Adding an API key 294
Checking, changing, or setting an API key 295
Viewing API Key Archive 296
Setting a TOTP authenticator 297
Removing a TOTP authenticator 298
Assets 298
Properties tab (asset) 302
Accounts tab (asset) 305
Account Dependencies tab (asset) 308
Access Request Policies (asset) 309
Owners tab (asset) 310
Discovered SSH Keys (asset) 311
Discovered Services tab (asset) 312
History tab (asset) 313
Managing assets 314
Adding an asset 315
Custom Properties 321
Checking an asset's connectivity 336
Assigning an asset to a partition 336
Assigning a profile to an asset 337
Manually adding a tag to an asset 337
Adding an account to an asset 338
Adding account dependencies 340
Adding users or user groups to an asset 341
Deleting an asset 341
Account Discovery tab (add asset) 342
Downloading a public SSH key 344
Partitions 345

About profiles ... 346
Properties tab (partitions) ... 347
Assets tab (partitions) ... 348
Accounts tab (partitions) ... 350
Owners tab (partitions) ... 353
Password Profiles tab (partitions) ... 354
SSH Key Profiles tab (partitions) ... 355
History tab (partitions) ... 356
Managing partitions ... 357
Adding a partition ... 358
Adding assets to a partition ... 358
Adding an account to a partition ... 359
Removing assets from a partition ... 360
Adding users or user groups to a partition ... 360
Creating a password profile ... 361
Creating an SSH key profile ... 362
Setting a default partition ... 362
Setting a default profile ... 363
Assigning assets or accounts to a password profile and SSH key profile ... 363
Deleting a partition ... 364
Discovery ... 364
Asset Discovery ... 365
Asset Discovery job workflow ... 367
Adding an Asset Discovery job ... 368
Deleting an Asset Discovery job ... 380
Asset Discovery Results ... 381
Account Discovery ... 381
Account Discovery job workflow ... 384
Adding an Account Discovery job ... 384
Deleting an Account Discovery job ... 391
Account Discovery Results ... 391
Discovered Accounts ... 392
Service Discovery Results ... 394
Discovered Services ... 395
SSH Key Discovery ... 398

SSH Key Discovery job workflow ... 400
Adding an SSH Key Discovery job ... 401
SSH Key Discovery Results ... 402
Discovered SSH Keys ... 403
Profiles ... 404
Password Profiles (profiles) ... 405
Properties tab (profiles) ... 406
Assets tab (profiles) ... 407
Accounts tab (profiles) ... 409
View Password Profile Components (profiles) ... 412
Managing password profiles ... 413
Adding a password profile ... 413
Password Profiles ... 414
Setting a default password profile ... 430
Deleting a password profile ... 430
SSH Key Profiles (profiles) ... 430
View SSH Key Profile Components (profiles) ... 431
Managing SSH key profiles ... 432
Adding an SSH key profile ... 432
SSH Key Profiles ... 433
Setting a default SSH key profile ... 449
Deleting an SSH key profile ... 449
Tags ... 449
Adding a tag for tagging of assets or asset accounts ... 451
Deleting an asset or asset account tag ... 456
Modifying an asset or asset account tag ... 457
Copying an asset or asset account tag to another partition ... 457
Viewing asset and asset account tag assignments ... 457
Registered Connectors ... 458
Adding a registered connector ... 459
Custom platforms ... 460
Creating a custom platform script ... 461
Adding a custom platform ... 462
Importing objects ... 462
Creating an import file ... 463

Template CSV file 464

Security Policy Management 467

Access Request Activity 467

Account Groups 468

Properties tab (account group) 469

Accounts tab (account group) 470

Access Request Policies tab (account group) 471

History tab (account group) 472

Managing account groups 473

Adding an account group 473

Adding a dynamic account group 474

Adding one or more accounts to an account group 477

Adding accounts to an access request policy 477

Deleting an account group 478

Application to Application 478

About Application to Application functionality 479

Setting up Application to Application 480

Adding an application registration 481

Deleting an application registration 483

Regenerating an API key 483

Making a request using the Application to Application service 484

Cloud Assistant 488

Adding authorized user for Cloud Assistant 489

Asset Groups 489

Properties tab (asset group) 490

Assets tab (asset group) 491

Access Request Policies tab (asset group) 492

History tab (asset group) 493

Managing asset groups 494

Adding an asset group 494

Adding a dynamic asset group 495

Adding assets to an asset group 497

Deleting an asset group 498

Entitlements 498

General tab (entitlements) 500

Users tab (entitlements) ... 500
Access Request Policies tab (entitlements) ... 501
History tab (entitlements) ... 502
Managing entitlements ... 504
Adding an entitlement ... 504
How SPP evaluates policy when a user submits an access request ... 505
Creating an access request policy ... 506
Adding users or user groups to an entitlement ... 517
Deleting an access request policy ... 517
Modifying an access request policy ... 518
Copying an access request policy ... 518
Deleting an entitlement ... 518
Linked Accounts ... 519
Users (linked accounts) ... 519
Accounts (linked accounts) ... 519
Managing linked accounts ... 520
Linking a user to an account ... 520
Linking an account to a user ... 521
Removing a linked account from a user ... 521
Removing a user from a linked account ... 521
User Groups ... 522
Properties tab (user groups) ... 523
Users tab (user groups) ... 523
Entitlements tab (user groups) ... 525
History tab (user groups) ... 526
Managing user groups ... 527
Adding a user group ... 527
Adding a directory user group ... 528
Adding users to a user group ... 531
Adding a user group to an entitlement ... 532
Deleting a user group ... 532
Security Policy Settings ... 533
Reasons ... 534

User Management ... 535
Users ... 535

Properties tab (user) ... 536
User Groups tab (user) ... 538
Entitlements tab (user) ... 539
History (user) ... 540
Managing users ... 541
Adding a user ... 541
Requiring secondary authentication log in ... 546
Adding a user to user groups ... 547
Adding a user to entitlements ... 547
Activating or deactivating a user account ... 548
Deleting a user ... 548
Setting a local user's password ... 548
Unlocking a local user's account ... 549
User Groups ... 549
Properties tab (user groups) ... 551
Users tab (user groups) ... 551
Entitlements tab (user groups) ... 553
History tab (user groups) ... 554
Managing user groups ... 555
Adding a user group ... 555
Adding a directory user group ... 556
Adding a SCIM user group ... 559
Adding users to a user group ... 560
Adding a user group to an entitlement ... 561
Deleting a user group ... 561
Time Zone ... 562

Reports ... 563
Activity Center ... 564
Applying search criteria ... 565
Saving search criteria and loading previously saved search criteria ... 566
Generating an activity audit log report ... 567
Scheduling an activity audit log report ... 567
Editing or deleting a saved search or scheduled report ... 569
Viewing event details ... 570
Auditing request workflow ... 570

Sorting report results ... 571
Entitlement reports ... 571
Exporting a detailed user entitlement report ... 572
Ownership reports ... 572

Disaster recovery and clusters ... 574
Enrolling replicas into a cluster ... 577
Considerations to enroll cluster members ... 577
Unjoining replicas from a cluster ... 578
Maintaining and diagnosing cluster members ... 580
About Offline Workflow Mode ... 581
Manually control Offline Workflow Mode ... 585
Failing over to a replica by promoting it to be the new primary ... 587
Activating a read-only appliance ... 588
Diagnosing a cluster member ... 588
Patching cluster members ... 589
About cluster patching ... 590
Using a backup to restore a clustered appliance ... 591
Resetting a cluster that has lost consensus ... 593
Performing a factory reset ... 595
Unlocking a locked cluster ... 597
Troubleshooting tips ... 598
Appliance states ... 599

Administrator permissions ... 604
Appliance Administrator permissions ... 604
Asset Administrator permissions ... 605
Auditor permissions ... 605
Authorizer Administrator permissions ... 606
Help Desk Administrator permissions ... 606
Operations Administrator permissions ... 607
Security Policy Administrator permissions ... 607
User Administrator permissions ... 608

Preparing systems for management ... 609
Preparing ACF - Mainframe systems ... 610
Preparing Amazon Web Services platforms ... 611

Preparing Cisco devices 611
Preparing Dell iDRAC devices 616
Preparing VMware ESXi hosts 616
Preparing Fortinet FortiOS devices 617
Preparing F5 Big-IP devices 617
Preparing HP iLO servers 617
Preparing HP iLO MP (Management Processors) 618
Preparing IBM i (AS/400) systems 618
Preparing JunOS Juniper Networks systems 619
Preparing MongoDB 619
Preparing MySQL servers 620
Preparing Oracle databases 620
Preparing PAN-OS (Palo Alto) networks 621
Preparing PostgreSQL 621
Preparing RACF mainframe systems 622
Preparing SAP HANA 622
Preparing SAP Netweaver Application Servers 623
Preparing Safeguard for Privileged Sessions for credential management 624
Preparing Sybase (Adaptive Server Enterprise) servers 625
Preparing SonicOS devices 625
Preparing SonicWALL SMA or CMS appliances 625
Preparing SQL Servers 626
Preparing Top Secret mainframe systems 627
Preparing Unix-based systems 628
Preparing Windows systems 629
Preparing WinRM systems 631
Preparing Windows SSH systems 632
VMware vCenter Server 633
Minimum required permissions for Windows assets 633

Troubleshooting 636
Appliance is sick 637
Connectivity failures 638
Change password or SSH key fails 638
Incorrect authentication credentials 639
Missing or incorrect SSH host key 639

No cipher supported error ... 640
Service account has insufficient privileges ... 640
Cannot connect to remote machine through SSH or RDP ... 641
Cannot delete account ... 641
Cannot play session message ... 641
Domain user denied access to SPP ... 642
LCD status messages ... 642
Appliance LCD and controls ... 643
My Mac keychain password or SSH key was lost ... 644
Password fails for Unix host ... 644
Password or SSH key is pending a reset ... 645
Password or SSH key profile did not run ... 645
Recovery Kiosk (Serial Kiosk) ... 646
Appliance information (Recovery Kiosk) ... 647
Backups ... 648
Power options ... 649
Rebooting the appliance ... 649
Shutting down the appliance ... 650
Admin password reset ... 650
Factory reset from the Recovery Kiosk ... 651
Support bundle ... 652
Replica not adding ... 653
System services did not update or restart after password or SSH key change ... 653
Test Connection failures ... 653
Test Connection failures on archive server ... 654
Certificate issue ... 654
Cipher support ... 654
Domain controller issue ... 656
Networking issue ... 656
Windows WMI connection ... 656
Timeout errors causing operations to fail ... 657
User locked out ... 657
User not notified ... 657

Frequently asked questions ... 658
How do I audit transaction activity ... 658

How do I configure external federation authentication 659
How do I add an external federation provider trust 660
How do I create a relying party trust for the STS 661
How do I add an external federation user 662
How do I manage accounts on unsupported platforms 663
How do I modify the appliance configuration settings 664
How do I prevent SPP messages when making RDP connections 665
How do I set up telnet and TN3270/TN5250 session access requests 667
How do SPP database servers use SSL 669
ODBC Transport 669
Microsoft SQL Server 669
MySQL Server 670
Sybase ASE Server 671
What are the access request states 672
What do I do when an appliance goes into quarantine 672
When does the rules engine run for dynamic grouping and tagging 675
Why did the password or SSH key change during an open request 675
Appendix: Safeguard ports 676
Appendix: SPP and Safeguard for Privileged Sessions appliance link guidance 684
Appendix: Regular expressions 688
About us 690
Contacting us 691
Technical support resources 692

1

Introduction

The One Identity Safeguard for Privileged Passwords Administration Guide is intended for IT administrators, Unix Administrators, Security Administrators, System Auditors, and other IT professionals who are installing and configuring One Identity Safeguard for Privileged Passwords for the first time.

NOTE: The term "Unix" is used informally in the SPP documentation to denote any operating system that closely resembles the trademarked system, Unix.

Introduction to One Identity Safeguard for Privileged Passwords

The One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance are built specifically for use only with the SPP privileged management software, which is pre-installed and ready for immediate use. The appliance is hardened to ensure the system is secured at the hardware, operating system, and software levels. The hardened appliance approach protects the privileged management software from attacks while simplifying deployment and ongoing management and shortening the time frame to value.

SPP virtual appliances and cloud applications are also available. When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. See One Identity's Product Support Policies for more information on environment virtualization.

Safeguard privileged management software suite

Safeguard privileged management software is used to control, monitor, and govern privileged user accounts and activities to identify possible malicious activities, detect entitlement risks, and provide tamper proof evidence. The Safeguard products also aid incident investigation, forensics work, and compliance efforts.

The Safeguard products' unique strengths are:

- One-stop solution for all privileged access management needs
- Easy to deploy and integrate
- Unparalleled depth of recording
- Comprehensive risk analysis of entitlements and activities
- Thorough Governance for privileged account

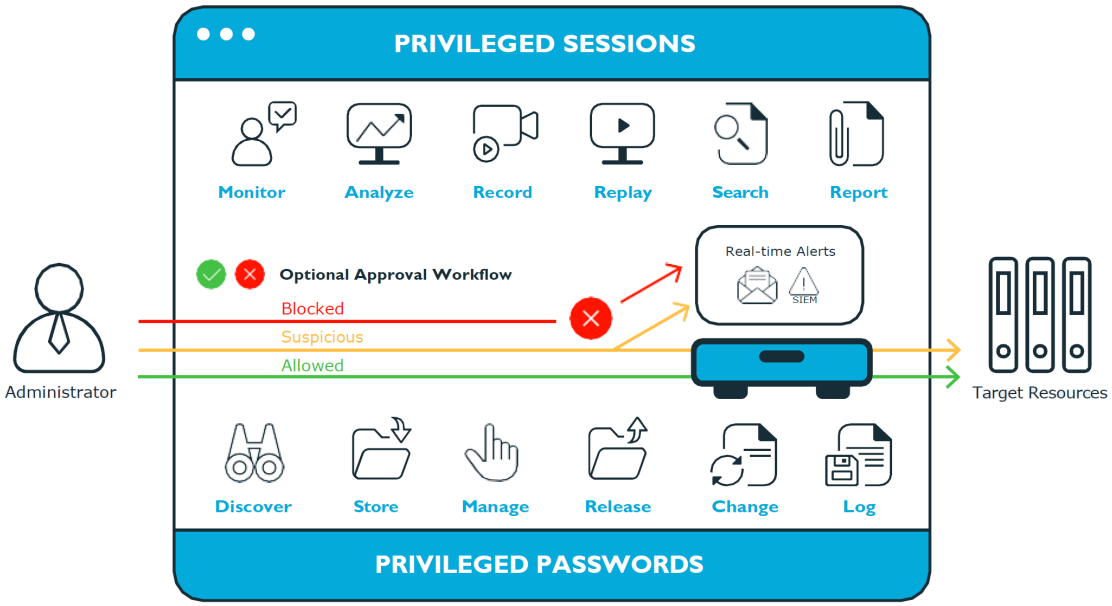
The suite includes the following modules:

- **One Identity Safeguard for Privileged Passwords** automates, controls, and secures the process of granting privileged credentials with role-based access management and automated workflows. Deployed on a hardened appliance, SPP eliminates concerns about secured access to the solution itself, which helps to speed integration with your systems and IT strategies. Plus, its user-centered design means a small learning curve and the ability to manage passwords from anywhere and using nearly any device. The result is a solution that secures your enterprise and enables your privileged users with a new level of freedom and functionality.
- **One Identity for Privileged Sessions** is part of One Identity's Privileged Access Management portfolio. Addressing large enterprise needs, Safeguard for Privileged Sessions is a privileged session management solution, which provides industry-leading access control, as well as session monitoring and recording to prevent privileged account misuse, facilitate compliance, and accelerate forensics investigations.

  Safeguard for Privileged Sessions is a quickly deployable enterprise appliance, completely independent from clients and servers to integrate seamlessly into existing networks. It captures the activity data necessary for user profiling and enables full user session drill-down for forensics investigations.

  > NOTE: Configuration options and details related to Safeguard for Privileged Sessions will only be visible to customers that have purchased and joined the product to One Identity Safeguard for Privileged Passwords.
- **One Identity Safeguard for Privileged Analytics** integrates data from Safeguard for Privileged Sessions to use as the basis of privileged user behavior analysis. Safeguard for Privileged Analytics uses machine learning algorithms to scrutinize behavioral characteristics, and generates user behavior profiles for each individual privileged user. Safeguard for Privileged Analytics compares actual user activity to user profiles in real time, and profiles are continually adjusted using machine learning. Safeguard for Privileged Analytics detects anomalies and ranks them based on risk so you can prioritize and take appropriate action and ultimately prevent data breaches.

Figure 1: Privileged Sessions and Privileged Passwords



Overview of the entities

Safeguard for Privileged Passwords is a password, keys, and secrets vault to secure assets including computers, servers, network devices, directories, and applications.

A high-level introduction to the Safeguard for Privileged Passwords entities and how they relate follows.

Assets, partitions, and profiles

Assets include computers, servers, network devices, directories, or applications for Safeguard to manage. Assets have associated user accounts and service accounts. Assets and accounts may be imported (for example, from Active Directory). Assets may or may not be part of an asset group.

The partition is a container for delegated management for account passwords and SSH keys (including check and change). Partitions are also useful to segregate assets to various owners to achieve Separation of Duties (SoD). Partitions allow you to set up multiple asset managers, each with the ability to define password guidelines for the managed systems in their own workspace. Typically you would partition assets by geographical location, owner, function, or by operating system. For example, you can group Unix assets in a partition and delegate the Unix administrator to manage it. Every partition should have a partition owner.

An asset can be assigned to only one partition at a time. When you assign an asset to a partition, all accounts associated with that asset are automatically reassigned to that partition, as well. Then, any new accounts you add for that asset are automatically assigned to that partition.

The profile includes the schedules and rules governing the partition’s assigned assets and the assets' accounts. For example, the profile defines how often a password check is required on an asset or account.

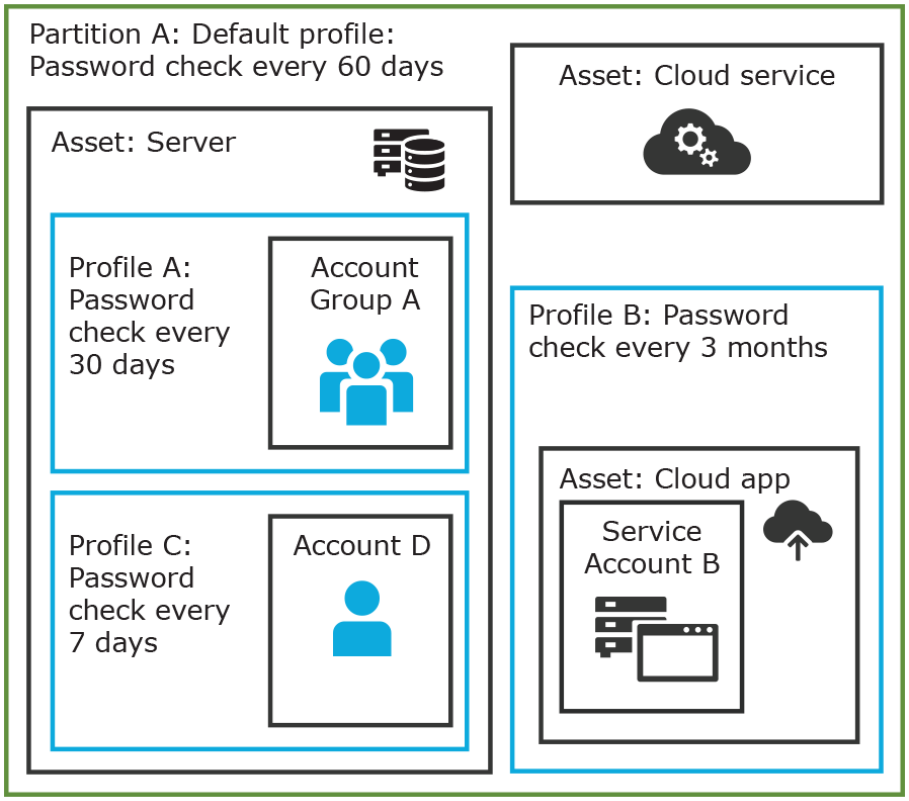
A partition can have multiple profiles, each assigned to different assets, if desired. An account is governed by only one profile. If an account is not explicitly assigned to a profile, the account is governed by the one assigned to the parent asset. If that asset does not have an assigned profile, the partition's default profile is assigned. When updating or restarting a service on a password change, the profile assigned to the asset is used for dependent account service modifications.

When you create a new partition, SPP creates a corresponding default profile with default schedules and rules. You can create multiple profiles to govern the accounts assigned to a partition. Both assets and accounts are assigned to the scope of a profile.

For example, suppose you have an asset with 12 accounts and you configure the profile to check and change passwords every 60 days. If you want the password managed for one of those accounts every seven days, you can create another profile and add the individual account to the new profile. Now, SPP will check and change all the passwords on this asset every 60 days except for this account, which will change every seven days.

In the example below, Partition A has three profiles (Profile A, B, and C) and a default profile. Profile A checks passwords every 30 days. Profile B checks passwords every three months, and Profile C has the highest level of security, checking passwords every seven days. Note that the asset Server has two profiles each governing different accounts associated with the asset. Profiles A, B, and C are all explicitly assigned to the accounts and assets shown. Asset cloud service doesn't have an explicitly assigned profile so the default will be used to manage accounts on the asset.

Figure 2: Password control



Details: Assets and asset groups

- An asset may be a computer, server, network device, directory, or application.
- You can log in to an asset with more than one account, but an account can only be associated with one asset.
- If you select an asset for a profile, all accounts are included.
- An asset must be assigned to only one partition. An asset typically has a profile, but it is not mandatory.
- You can create multiple assets for the same device or application then manage different accounts on each asset. For example, a directory asset can manage a subset of the forest.
- An asset group is a set of assets that can be added to the scope of an entitlement's access request policy.

Details: Partitions and profiles

- A partition is a group of assets (and the assets' associated accounts) governed by a profile and used to delegate asset management. An asset can only be in one partition at a time. All accounts associated with that asset are automatically added to the partition.

- Profiles are the schedules and rules that govern a partition's assets and the assets' accounts. You can set a default profile to assign or you can manually assign a profile to an asset or account.
- When a partition is created, a default profile is created for that partition. This profile is implicitly associated with all assets and accounts added to the partition. Later, a different profile can be manually assigned to assets and account which is referred to as an explicit association. Explicit associations (manual assignments) override implicit associations (auto-assignments).

Accounts, account groups, entitlements, and entitlement access request policies

Assets have associated accounts, like a user account or an account for a Windows service. An account can only be associated with one asset.

Entitlements grant access to users, user groups, or both. An entitlement includes one or more access request policies and may be related to job functions like help desk support or Unix administrators.

An entitlement access request policy defines what is managed by the policy and is referred to as the "scope of the policy." Different types of access requests include password, SSH keys, and sessions.

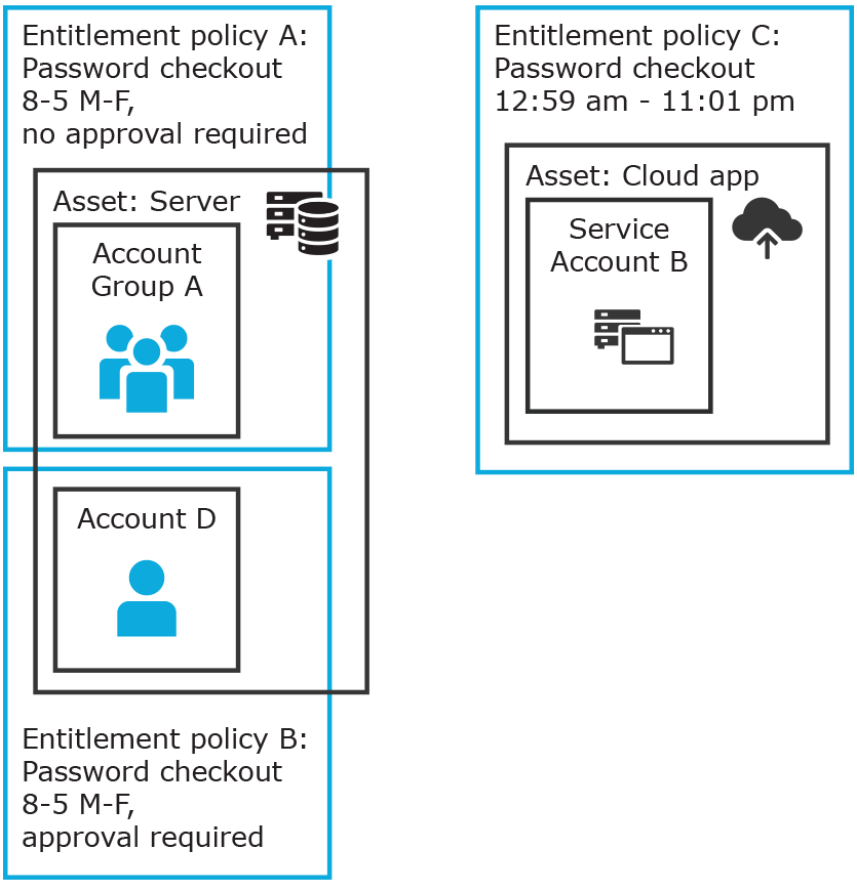
- To define an access request policy for a password or SSH key request, the valid properties in scope are accounts and account groups.
- To define an access request policy for a sessions request, the valid properties in scope are accounts, account groups, assets, and asset groups. If only assets or asset groups are defined in the access request policy, the **Asset Based Session Access** must have an option other than **None**.

Entitlement access request policies may include:

- The access type:
  - Credential access types include Password Release and SSH key
  - Sessions access types include the protocols Secure SHell (SSH), Remote Desktop Protocol (RDP), and Telnet
- The scope: Accounts, account groups, assets, and asset groups, as needed
- Requester settings: This includes a reason for the request, comment, ticket number (if applicable), and access duration
- Approver and Reviewer settings: If required, this includes the approvers and reviewers along with notifications
- Access configuration: Settings based on the type of access (Password, SSH key, SSH session, or RDP session set earlier)
- Session settings: Used for recording sessions, if you use Safeguard for Privileged Sessions
- Time restrictions: Days and hours of access, if you choose to set these
- Emergency settings: Who to contact, if you choose to specify this information

In the example below, each account or account group is assigned to only one asset. The Server asset is associated with Account D and Account Group A which is made up of several accounts. Entitlement access request policy A is assigned to Account Group A so that group can check out passwords from 8 a.m. to 5 p.m. on Monday through Friday with no approval required. Entitlement access request policy B, which is associated with Account D, allows for password check out for the same time frame, but the check outs require approvals. Entitlement access request policy C allows for password check out from 12:59 a.m. to 11:01 p.m. to allow for the system maintenance window.

Figure 3: Entitlements and accounts



Details: Accounts and account groups

- An account can only be associated with one asset.
- An account group is a set of accounts that can be added to the scope of an entitlement's access request policy. An account group can span multiple assets.
- Directory accounts are associated with assets that are directories.
- Both directory accounts and directory assets can can be visible or "shared" across partition boundaries, for specific purpose. Directory assets can be shared for Asset Discovery jobs. Directory accounts can be used as a service account or dependent account to a Windows service or task.

Details: Entitlements and access request policies

- An entitlement is a set of access request policies that restrict resources, typically by job role.
- Entitlements are used to authorize users or members of user groups to access accounts in the scope of the set of the entitlement's access request policies. One entitlement may have zero, one, or multiple access request policies. Users and user groups can be added to entitlements.
- Access request policies contain the details of the type of access as well as conditions. For example, the type of access may include password versus session (RDP session, SSH client, other protocols), time limits, individual accountability (change after check-in), and other settings. Conditions may include number of approvers, time of day, ticketing system, reason codes, and so on. An access request policy can only be associated with one entitlement.
- Access request policies are scoped to resources. Sometimes that scoping is done directly to accounts and the asset is implied. Or, the scoping is done to the asset and the access request policy identifies the account.

Users and user groups

Users are individuals. A user may be assigned administrative permissions to govern assets, partitions, accounts, and entitlement access request policies. A user may be assigned more than one set of permissions by the Authorizer Administrator. It is a best practice to follow the principles of separation of duties (SoD) in administration assignments. For example, the assignment of Asset Administrator, Security Policy Administrator, User Administrator, and Auditor should be different users.

Standard users do not have administrative permissions. They can request access, approve access requests, or review completed access requests.

Users can be configured for two-factor authentication.

Details: Users and user groups

- A user is a person who can log into SPP. A user can be associated with an identity provider that is local or a user can be a directory user from an external identity store such as Microsoft Active Directory. A user may be associated with user groups, partitions, entitlements, and linked accounts.
- A user group is a set of users that can be added to an entitlement, typically based on roles. The user group's access is governed by the entitlement’s access request policies. Both local user groups and directory user groups can be added to SPP.
- A user can be assigned administrative permissions over assets, security, and so on. A standard user has no administrative permissions and performs other duties, for example, to approve access requests.

Discovery

You can discover assets and accounts that are not being managed so you can place them under management, if appropriate. Discovery jobs can be configured to discover assets and accounts.

Access request workflow

At a high-level, an end user or custom integration application may submit an access request for:

- A credential (password or SSH key) that is managed by Safeguard for Privileged Passwords
- A session (such as RDP, SSH, or Telnet) to an asset that is managed by Safeguard for Privileged Passwords with the addition of Safeguard for Privileged Sessions

The access request may immediately be granted, or it may first have to go through an approval process.

Once approved, the credential or session can be checked out and used. For sessions, all connections are proxied through Safeguard for Privileged Sessions and recorded.

After using the credentials or session, it can be checked in to signify that the user is done. The access request policy may then be configured such that a review of the request is required before it can be checked out again. For credential type requests, the access request policy may also be configured to change the credential.

Appliance specifications

The SPP Appliance is built specifically for use only with the SPP privileged management software that is already installed and ready for immediate use. It comes hardened to ensure the system is secure at the hardware, operating system, and software levels.

The following tables list the One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance specifications and power requirements.

Table 1: 4000 Appliance: Feature specifications

4000 Appliance	Feature / Specification
Processor	Intel Xeon 4310T 2.3 GHz
# of Processors	1
# of Cores per Processor	10 cores (20 threads)
L2/L3 Cache	15 MB Cache
Chipset	Intel C621A Chipset
DIMMs	ECC DDR4-2667
RAM	64 GB
Internal HD Controller	Supermicro AOC-S3908L-H8iR-16DD
Disk Hard Drive	4 x Seagate Exos 7E10 2TB SAS 512e

4000 Appliance	Feature / Specification
Availability	TPM 2.0, EEC Memory, Redundant PSU
I/O Slots	2x PCIe 4.0 x16 FHHL 1x PCIe 4.0 x16 HHHL
RAID	RAID10
NIC/LOM	Broadcom P210TP - 2 x 10G BASE-T Broadcom P210P - 2 x 10G SFP+
Power Supplies	Redundant, 500W/600W, Auto Ranging (100v~240V), RoHS and REACH compliant
Fans	6 Supermicro FAN-0141L
Chassis	1U Rack
Dimensions (HxWxD)	43 x 437.0 x 650.0 (mm) 1.7 x 17.2 x 25.6 (in)
Weight	Max: 37 lbs (16.78 Kg)

Table 2: 3000 Appliance: Feature specifications

3000 Appliance	Feature / Specification
Processor	Intel Xeon E3-1275v6 3.8 GHz
# of Processors	1
# of Cores per Processor	4 cores (8 threads)
L2/L3 Cache	8MB L3 Cache
Chipset	Intel C236 Chipset
DIMMs	Unbuffered ECC UDIMM DDR4 2400MHz
RAM	32 GB
Internal HD Controller	LSI MegaRAID SAS 9361-4i Single
Disk Hard Drive	4 x Seagate 7E2000 2TB SAS 512E
Availability	TPM 2.0, EEC Memory, Redundant PSU
I/O Slots	x16 PCIe 3.0, x8 PCIe 3.0
RAID	RAID10
NIC/LOM	4 port - dual GbE LAN with Intel i210-AT
Power Supplies	Redundant, 700W, Auto Ranging (100v~240V), ACPI compatible

3000 Appliance	Feature / Specification
Fans	1 Supermicro SNK-P0046P and 2 Micron 16GB 2666MHz 2R ECC Unb Z01B Dual Label
Chassis	1U Rack
Dimensions (HxWxD)	43 x 437.0 x 597.0 (mm) 1.7 x 17.2 x 23.5 (in)
Weight	Max: 37 lbs (16.78 Kg)

Table 3: 2000 Appliance: Feature specifications

2000 Appliance	Feature / Specification
Processor	Intel Xeon E3-1275v5 3.60 GHz
# of Processors	1
# of Cores per Processor	4
L2/L3 Cache	4 x 256KB L2, 8MB L3 SmartCache
Chipset	Intel C236 Chipset
DIMMs	DDR4-2400 ECC Unbuffered DIMMs
RAM	32GB
Internal HD Controller	LSI MegaRAID SAS 9391-4i 12Gbps SAS3
Disk	4 x Seagate EC2.5 1TB SAS 512e
Availability	TPM 2.0, EEC Memory, Redundant PSU
I/O Slots	x16 PCIe 3.0, x8 PCIe 3.0
RAID	RAID10
NIC/LOM	3 x Intel i210-AT GbE
Power Supplies	Redundant, 700W, Auto Ranging (100v~240V), ACPI compatible
Fans	4 x 40mm Counter-rotating, Non-hot-swappable
Chassis	1U Rack
Dimensions (HxWxD)	43 x 437.0 x 597.0 (mm) 1.7 x 17.2 x 23.5 (in)
Weight	Max: 46 lbs (20.9 Kg)
Miscellaneous	FIPS Compliant Chassis

Table 4: One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance: Power requirements

Input Voltage	100-240 Vac
Frequency	50-60Hz
Power Consumption (Watts)	170.9
BTU	583

SPP is also available as a virtual appliance and from the cloud. For details see:

- Using the virtual appliance and web management console
- Cloud deployment considerations

2

System requirements and versions

One Identity Safeguard for Privileged Passwords allows you to manage access requests, approvals, and reviews for your managed accounts and systems.

- The web client consists of an end-user view and administrator view. The fully featured client exposes all of the functionality of Safeguard based on the role of the authenticated user.
- The web management console displays whenever you connect to the virtual appliance and is used for first time configuration.
  When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. See One Identity's Product Support Policies for more information on environment virtualization.

Ensure that your system meets the minimum hardware and software requirements for these clients.

If a Safeguard Sessions Appliance is linked to SPP, session recording is handled via Safeguard for Privileged Session. The link is initiated from Safeguard for Privileged Sessions. For details about the link steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide*.

Bandwidth

It is recommended that connection, including overhead, is faster than 10 megabits per second inter-site bandwidth with a one-way latency of less than 500 milliseconds. If you are using traffic shaping, you must allow sufficient bandwidth and priority to port 655 UDP in the shaping profile. These numbers are offered as a guideline only in that other factors could require additional network tuning. These factors include but are not limited to: jitter, packet loss, response time, usage, and network saturation. If there are any further questions, please check with your Network Administration team.

Web client system requirements

Table 5: Web requirements

Component	Requirements
Web browsers	Desktop browsers: • Apple Safari 16.0 for desktop (or later) • Google Chrome 108 (or later) • Microsoft Edge 108 (or later) • Mozilla Firefox 108 (or later) Mobile device browsers: • Apple Safari Mobile 14.7 (or later) • Google Chrome on Android 108 (or later)

Web management console system requirements

Table 6: Web kiosk requirements

Component	Requirements
Web management console	Desktop browsers: • Apple Safari 16.0 for desktop (or later) • Google Chrome 108 (or later) • Microsoft Edge 108 (or later) • Mozilla Firefox 108 (or later)

Platforms and versions follow.

- You must license the VM with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative.
- Supported hypervisors:
  - Microsoft Hyper-V (VHDX) version 8 or higher
  - VMware vSphere with vSphere Hypervisor (ESXi) versions 6.5 or higher
  - VMware Workstation version 13 or higher

- Minimum resources: 4 CPUs, 10GB RAM, and a 500GB disk. The virtual appliances default deploy does not provide adequate resources. Ensure these minimum resources are met.

Supported platforms

One Identity Safeguard for Privileged Passwords supports a variety of platforms, including custom platforms.

SPP tested platforms

The following table lists the platforms and versions that have been tested for SPP (SPP). Additional assets may be added to SPP. If you do not see a particular platform listed when adding an asset, use the **Other**, **Other Managed**, **Other Directory**, or **Linux** selection on the **Management** tab of the **Asset** dialog. For more information, see Management tab (add asset).

SPP linked to Safeguard for Privileged Sessions: Sessions platforms

CAUTION: When linking your Safeguard for Privileged Sessions (SPS) deployment to your SPP (SPP) deployment, ensure that the SPS and SPP versions match exactly, and keep the versions synchronized during an upgrade. For example, you can only link SPS version 6.6 to SPP version 6.6, and if you upgrade SPS to version 6.7, you must also upgrade SPP to 6.7.

Make sure that you do not mix Long Term Supported (LTS) and feature releases. For example, do not link an SPS version 6.0.1 to an SPP version 6.1.

When One Identity Safeguard for Privileged Passwords (SPP) is linked with a Safeguard for Privileged Sessions (SPS) appliance, platforms are supported that use one of these protocols:

- SPP 2.8 or lower: RDP, SSH
- SPP 2.9 or higher: RDP, SSH, or Telnet

Some platforms may support more than one protocol. For example, a Linux (or Linux variation) platform supports both SSH and Telnet protocols.

Table 7: Supported platforms: Assets that can be managed

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
ACF2 - Mainframe	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
ACF2 - Mainframe LDAP	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	False
Active Directory	Active Directory	True	False
AIX	AIX 7.2 AIX 7.3	True	True
Amazon Linux	Amazon Linux 2 Amazon Linux 2022 Amazon Linux Other	True	True
Amazon Web Services	Amazon Web Services 1	True	False
CentOS Linux	CentOS Linux 7 CentOS Linux 8	True	True
Check Point GAiA (SSH)	Check Point GAiA (SSH) R80.30 Check Point GAiA (SSH) R81	True	True
Cisco ASA	Cisco ASA 7.X Cisco ASA 8.X Cisco ASA 9.X	True	True
Cisco IOS (510)	Cisco IOS 12.X Cisco IOS 15.X Cisco IOS 16.X	True	True
Cisco ISE	Cisco ISE 2.7 Cisco ISE 3	True	False
Cisco ISE CLI	Cisco ISE CLI 2.7 Cisco ISE CLI 3	True	True
Cisco NX-OS	Cisco NX-OS 9.3(7) Cisco NX-OS 9.3(7a)	True	True
Debian GNU/Linux	Debian GNU/Linux 10 Debian GNU/Linux 11 Debian GNU/Linux 12	True	True
Dell iDRAC	Dell iDRAC 8	True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
	Dell iDRAC 9		
eDirectory LDAP	eDirectory LDAP 9.0	True	False
ESXi	ESXi 7.0 ESXi 8.0	True	False
F5 Big-IP	F5 Big-IP 12.1.2 F5 Big-IP 13.0 F5 Big-IP 14.0 F5 Big-IP 15.0	True	True
Fedora	Fedora 37 Fedora 38	True	True
Fortinet FortiOS	Fortinet FortiOS 6.2 Fortinet FortiOS 6.4 Fortinet FortiOS 7.0 Fortinet FortiOS 7.2 Fortinet FortiOS 7.4	True	True
FreeBSD	FreeBSD 12 FreeBSD 13	True	True
HP iLO	HP iLO 4 HP iLO 5 HP iLO 6	True	True
HP iLO MP	HP iLO MP 2 HP iLO MP 3	True	True
HP-UX	HP-UX 11iv3 (B.11.31)	True	True
IBM i	IBM i 7.3 IBM i 7.4	True	True
Junos - Juniper Networks	Junos - Juniper Networks 19 Junos - Juniper Networks 20 Junos - Juniper Networks 21 Junos - Juniper Networks 22	True	True
LDAP	OpenLDAP 2.4	True	False

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
Linux		True	True
macOS	macOS 11 macOS 12 macOS 13	True	True
MongoDB	MongoDB 4.4 MongoDB 5.0 MongoDB 6.0	True	False
MySQL	MySQL 5.7 MySQL 8.0 MySQL 8.1	True	False
Oracle	Oracle 19c Oracle 21c	True	False
Oracle Linux (OL)	Oracle Linux (OL) 7 Oracle Linux (OL) 8 Oracle Linux (OL) 9	True	True
Other		False	False
Other Directory		True	False
Other Managed		True	False
PAN-OS	PAN-OS 9.1 PAN-OS 10.1 PAN-OS 10.2	True	True
PostgreSQL	PostgreSQL 11 PostgreSQL 12 PostgreSQL 13 PostgreSQL 14 PostgreSQL 15	True	False
RACF - Mainframe	RACF - Mainframe z/OS V2.1 Security Server zSeries RACF - Mainframe z/OS V2.2 Security Server zSeries RACF - Mainframe z/OS V2.3 Security	True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
	Server zSeries		
RACF - RACF - Mainframe LDAP	RACF - Mainframe LDAP z/OS V2.1 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.2 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.3 Security Server zSeries	True	False
Red Hat Enterprise Linux (RHEL)	Red Hat Enterprise Linux (RHEL) 7 Red Hat Enterprise Linux (RHEL) 8 Red Hat Enterprise Linux (RHEL) 9	True	True
Red Hat Directory Server	Red Hat Directory Server 11 Red Hat Directory Server 12	True	False
SAP HANA	SAP HANA SAP HANA 2	True	False
SAP Netweaver Application Server	SAP Netweaver Application Server 7.5	True	False
Safeguard for Privileged Sessions	Safeguard for Privileged Sessions 7.0	True	True
Solaris	Solaris 10 Solaris 11.3 Solaris 11.4	True	True
SonicOS	SonicOS 6.5 SonicOS 7 SonicOSX 7	True	False
SonicWALL SMA or CMS	SonicWALL SMA or CMS 11.3.0	True	False
SQL Server	SQL Server 2012 SQL Server 2014 SQL Server 2016 SQL Server 2017 SQL Server 2019 SQL Server 2022	True	False

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
SUSE Linux Enterprise Server (SLES)	SUSE Linux Enterprise Server (SLES) 12 SUSE Linux Enterprise Server (SLES) 15	True	True
Sybase (Adaptive Server Enterprise)	Sybase (Adaptive Server Enterprise) 15.7 Sybase (Adaptive Server Enterprise) 16 Sybase (Adaptive Server Enterprise) 17	True	False
Top Secret - Mainframe	Top Secret - Mainframe r14 zSeries Top Secret - Mainframe r15 zSeries Top Secret - Mainframe r16 zSeries	True	False
Top Secret - Mainframe LDAP	Top Secret - Mainframe LDAP r14 Top Secret - Mainframe LDAP r15 Top Secret - Mainframe LDAP r16	True	True
Ubuntu	Ubuntu 18.04 LTS Ubuntu 22.04 LTS Ubuntu 22.10 Ubuntu 23.04	True	True
VMware vCenter Server	VMware vCenter Server 6.7 VMware vCenter Server 7.0	True	True
Windows Desktop Windows Desktop (SSH) Windows Desktop (WinRM) Windows Server Windows Server (SSH) Windows Server (WinRM)	Windows (SSH) 10 Windows (SSH) 11 Windows (SSH) Server 2012 Windows (SSH) Server 2012 R2 Windows (SSH) Server 2016 Windows (SSH) Server 2019 Windows (SSH) Server 2022 Windows 10 Windows 11 Windows Server 2012 Windows Server 2012 R2	True	True

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
	Windows Server 2016 Windows Server 2019 Windows Server 2022		

Table 8: Supported platforms: Directories that can be searched

Platform Name	Platform Version
Microsoft Active Directory	Windows 2008+ DFL/FFL
LDAP	2.4

For all supported platforms, it is assume that you are applying the latest updates. For unpatched versions of supported platforms, Support will investigate and assist on a case by case basis but it may be necessary for you to upgrade the platform or use SPP's custom platform feature.

IMPORTANT: For the current list of platforms supported by Connect for Safeguard Assets, see the *Connect for Safeguard Assets User Guide*.

Custom platforms

The following example platform scripts are available:

- Custom HTTP
- Linux SSH
- Telnet
- TN3270 transports are available

For more information, see Custom platforms and Creating a custom platform script. Custom Platforms and Creating a custom platform script in the *Safeguard for Privileged Passwords Administration Guide*.

Sample custom platform scripts and command details are available at the following links available from the Safeguard Custom Platform Home wiki on GitHub:

- Command-Reference:

  https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Command-Reference
- Writing a custom platform script:

  https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/WritingACustomPlatformScript
- Example platform scripts are available at this location:

https://github.com/OneIdentity/SafeguardCustomPlatform/tree/master/SampleScripts

CAUTION: Example scripts are provided for information only. Updates, error checking, and testing are required before using them in production. SPP checks to ensure the values match the type of the property that include a string, boolean, integer, or password (which is called secret in the API scripts). SPP cannot check the validity or system impact of values entered for custom platforms.

Licenses

As a SPP user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

Hardware appliance

The One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance ship with the Privileged Passwords module which requires a valid license to enable functionality.

You must install a valid license. Once the module is installed, SPP shows a license state of **Licensed** and is operational. If the module license is not installed, you have limited functionality. That is, even though you will be able to configure access requests, if a Privileged Passwords module license is not installed, you will not be able to request a password release.

Virtual appliance Microsoft Windows licensing

You must license the virtual appliance with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative. The virtual appliance will not function unless the operating system is properly licensed.

Licensing setup and update

To enter licensing information when you first log in

The first time you log in as the Appliance Administrator, you are prompted to add a license. The **Success** dialog displays when the license is added.

On the virtual appliance, the license is added as part of Initial Setup. For more information, see Setting up the virtual appliance on page 52.

IMPORTANT: After successfully adding a license, the Software Transaction Agreement will be displayed and must be read and accepted in order to use SPP.

To configure reminders for license expiration

To avoid disruptions in the use of SPP, the Appliance Administrator must configure the SMTP server, and define email templates for the `License Expired` and the `License Expiring Soon` event types. This ensures you will be notified of an approaching expiration date. For more information, see Enabling email notifications on page 219.

Users are instructed to contact their Appliance Administrator if they get an "appliance is unlicensed" notification.

As an Appliance Administrator, if you receive a "license expiring" notification, apply a new license.

To update the licensing file

Safeguard licenses can be updated both on hardware and virtual machines, whereas OS licenses can be updated only on virtual machines.

To perform licensing activities

Navigate to **Appliance Management** > **Appliance** > **Licensing**.

- To upload a new license file, click **+ Upload new license file** and browse to select the current license file. The Software Transaction Agreement will also be displayed during this process and must be read and accepted in order to complete the licensing process.
- To remove the license file, select the license and click **Remove selected license**.
- To get more information on the license and to export license data, click the **What do these numbers mean?** button, or click on the numbers in the tile.

  If you want to export data about users, desktops or systems in CSV or JSON format, navigate to the table from which you want to export data by clicking the corresponding tab, for example **Users Used**.

  Click the export icon located on the table. For more information on exporting, see Exporting data.

  Below is the list of the available tabs.

  For device-based licenses:

  - General
  - Desktops Used
  - Other Desktops
  - Systems Used
  - Other Systems
  - History

  For user-based licenses:

  - General
  - Users Used

    - Password Vault Only
    - Other Users
    - History
- The **General** tab, contains general information about the license:
    - License usage and consumption
    - Counts of all managed and unmanaged components
    - How licenses are counted
    - License Number
    - License Type
    - Expiration Date
    - Product Version
    - Date Added
    - Added By

Long Term Support (LTS) and Feature Releases

Releases use the following version designations:

- Long Term Support (LTS) Releases: The first digit identifies the release and the second is a zero (for example, 6.0 LTS).
- Maintenance LTS Releases: A third digit is added followed by LTS (for example, 6.0.6 LTS).
- Feature Releases: The Feature Releases version numbers are two digits (for example, 6.6).

Customers choose between two paths for receiving releases: Long Term Support (LTS) Release or Feature Release. See the following table for details.

Table 9: Comparison of Long Term Support (LTS) Release and Feature Release

	Long Term Support (LTS) Release	Feature Release
General Release	**Scope**: Includes new features, resolved issues and security updates **Versioning**: The first digit identifies the LTS and the second digit is a 0 (for	**Scope**: Includes the latest features, resolved issues, and other updates, such as security patches for the OS **Versioning**: The first digit identifies the LTS and the second digit is a number identifying the Feature

	example, 6.0 LTS, 7.0 LTS, and so on).	Release (for example, 6.6, 6.7, and so on).
Maintenance Release	**Scope**: Includes critical resolved issues **Versioning**: A third digit designates the maintenance LTS Release (for example, 6.0.6 LTS).	**Scope**: Includes highly critical resolved issues **Versioning**: A third digit designates the maintenance Feature Release (for example, 6.6.1).

Release and support details can be found at Product Life Cycle.

CAUTION: Downgrading from the latest Feature Release, even to an LTS release, voids support for SPP.

One Identity strongly recommends always installing the latest revision of the release path you use (Long Term Support path or Feature Release path).

Moving between LTS and Feature Release versions

You can move from an LTS version (for example, 6.0.7 LTS) to the same feature version (6.7) and then patch to a later feature version. After that, you can patch from the minimum version for the patch, typically N-3. If you move from an LTS version to a feature version, you will receive a warning like the following which informs you that you will only be able to apply a Feature Release until the next LTS Release:

```
Warning: You are patching to a Feature Release from an LTS Release. If you
apply this update, you will not be able to upgrade to a non-Feature Release
until the next LTS major release version is available. See the Administration
Guide for details.
```

You cannot move from a Feature Release to LTS Release. For example, you cannot move from 6.7 to 6.0.7 LTS. You have to keep upgrading with each new Feature Release until the next LTS Release version is published. For this example, you would wait until 7.0 LTS is available.

Patching

You can only patch from a major version. For example, if you have version 6.6 and want to patch to 7.7, you must patch to 7.0 LTS and then apply 7.7.

An LTS major version of One Identity Safeguard for Privileged Passwords (SPP) will only work with the same LTS major version of Safeguard for Privileged Sessions (SPS). For the best experience, it is recommended you use the latest supported version.

3

Using API and PowerShell tools

SPP has a robust API with an easy to use tutorial. Safeguard PowerShell can be used to automate functions.

Using the API

Using Safeguard PowerShell

Using the API

Safeguard for Privileged Passwords (SPP) is built with an API-first design and uses a modernized API based on a REST architecture which allows other applications and systems to interact with it. Every function is exposed through the API to enable quick and easy integration regardless of what action you perform or in which language your applications are written. There are even a few things that can only be performed via the Safeguard SPP API.

CAUTION: Starting with SPP 6.8, any user that built a custom solution that monitors for events using ASP.NET SignalR will need to make changes to their solutions due to the upgrade to ASP.NET Core SignalR. For more information on this change and how to upgrade between the two versions, see the Microsoft documentation.

Users that built custom solutions that do not rely on event monitoring via SignalR should not be impacted.

NOTE: SPP 6.8 versions of open source projects hosted on GitHub (SafeguardDotNet, SafeguardJava, safeguard-bash) have been updated to support ASP.NET Core SignalR so they will work with the new SignalR changes in SPP 6.8.

API tutorial

The SPP API tutorial is available on GitHub at: https://github.com/oneidentity/safeguard-api-tutorial.

Access the SPP API

SPP has the following API categories:

- **Core**: Most product functionality is found here. All cluster-wide operations: access request workflow, asset management, policy management, and so on.

  `https://<Appliance IP>/service/core/swagger/`

- **Appliance**: RAppliance-specific operations, such as setting IP address, maintenance, backups, support bundles, appliance management.

  `https://<Appliance IP>/service/appliance/swagger/`

- **Notification**: Anonymous, unauthenticated operations. This service is available even when the appliance isn't fully online.

  `https://<Appliance IP>/service/notification/swagger/`

- **Event**: Specialized endpoint for connecting to SignalR for real-time events.

  `https<Appliance IP>event/signalr`

- **a2a**: Application integration specific operations. Fetching passwords and SSH keys, making access requests on behalf of users, and so on.

  `https://<Appliance IP>/service/a2a/swagger`

You must use a bearer token to access most resources in the API. When using the Swagger web UI (as referenced in the URLs above), click the **Authorize** button at the top of each page and log in using the web UI. The Swagger web UI adds the bearer token to each API request automatically. However, if you are manually making the API request or writing your own application/script, perform the following two steps to obtain a bearer token.

1. You must first authenticate using the OAuth 2.0 **Resource Owner Password Credentials** or **Client Credentials** grant types.

   An example of **Resource Owner Password Credentials** is:

```
POST https://<ApplianceIP>/RSTS/oauth2/token
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json

{
    "grant_type": "password",
    "username": "<Username>",
    "password": "<Password>",
    "scope": "rsts:sts:primaryproviderid:local"
}
```

   Where:

- `grant_type` is required and must be set to `password`.
- `username` is required and set to the user account you want to log in as.
- `password` is required and set to the password associated with the username.
- `scope` is required and set to one of the available identity provider's scope ID. The value shown in the example request, `rsts:sts:primaryproviderid:local`, is the default value available on all SPP Appliances. User accounts that you create in SPP directly (that is, not an Active Directory or LDAP account) will most likely have this scope value.

  > NOTE: The list of identity providers is dynamic and their associated scope ID can only be obtained by making a request to:
  >
  > `https://<ApplianceIP>/service/core/v4/AuthenticationProviders`
  >
  > and parsing the returned JSON for the `RstsProviderScope` property.

  > NOTE: Certain OAuth 2.0 grant types can be disabled if they are not needed. For more information, see Local Login Control.

  If you wish to authenticate using a client certificate, you must use the OAuth 2.0 **Client Credentials** grant type in which your certificate is included as part of the SSL connection handshake and the `Authorization` HTTP header is ignored. Set the `scope` to `rsts:sts:primaryproviderid:certificate` or any other identity provider that supports client certificate authentication.

```
POST https://<ApplianceIP>/RSTS/oauth2/token
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json

{
    "grant_type": "client_credentials",
    "scope": "rsts:sts:primaryproviderid:certificate"
}
```

2. After successfully authenticating, your response will contain an `access_token` that must be exchanged for a user token to access the API.

```
POST https://<ApplianceIP>/service/core/v4/Token/LoginResponse
Host: <ApplianceIP>
Content-Type: application/json
Accept: application/json

{
    "StsAccessToken": "<access_token from previous response>"
}
```

You should now have an authorization token to be used for all future API requests. The token is to be included in the HTTP `Authorization` header as a `Bearer` token like this:

```
Authorization: Bearer <UserToken value>
```

For example:

```
GET https://<ApplianceIP>/service/core/v4/Users/-2
Host: <ApplianceIP>
Accept: application/json
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1Ni...
```

NOTE: The token will expire in accordance to the **Token Lifetime** setting that is configured in SPP at the time the token was issued.

Customize the response using API query parameters

You can use the following API query parameters to customize the response returned from the API.

The following output parameters allow you to define the property names to be included and the property names to be used for sorting.

Table 10: API query filtering: Output

Output	Example	Description/Notes
`fields`	`GET /Users?fields=FirstName,LastName`	List of property names to be included in the output.
`orderby`	`Get /AssetAccounts?orderby=-AssetName,Name`	List of property names to be used to sort the output. Implies descending order.

The following paging parameters allow you to include an item count, the starting page, and the number of items per page.

Table 11: API query filtering: Paging

Paging	Example	Description/Notes
`count`	`GET /Assets?count=true`	Indicates, True or False, whether to return a single integer value representing the total number of items that match the given criteria.

Paging	Example	Description/Notes
`page & limit`	`GET /DirectoryAccounts?page=3&limit=100`	`page` defines which page (starting with 0) of data to return. `limit` defines the size of the page data.

The following operators can be used to filter the results.

Table 12: API query filtering: `filter` parameter

Operator	Example	Description/Notes
`eq`	`GET /AssetAccounts?filter=Name eq 'George'`	equal to
`ne`	`GET /Users?filter=LastName ne 'Bailey'`	not equal to
`gt`	`GET /Assets?filter=Id gt 10`	greater than
`ge`	`GET /Assets?filter=Id ge 10`	greater than or equal to
`lt`	`GET /Assets?filter=Id lt 10`	less than
`le`	`GET /Assets?filter=Id le 10`	less than or equal to
`and`	`GET /UserGroups?filter=(Id eq 1) and (Name eq 'Angels')`	both operands return true
`or`	`GET /UserGroups?filter=(Id eq 1) or (Name eq 'Bedford')`	at least one operand returns true
`not`	`GET /UserGroups?filter=(Id eq 1) and not (Name eq 'Potters')`	narrows the search by excluding the "not" value from the results
`contains`	`GET /Users?filter=Description contains 'greedy'`	contains the word or phrase
`q`	`GET /Users?q=bob`	`q` can be used to search across text properties; means "contains" for all relevant properties.
`in`	`GET /Users?filter=UserName in [ 'bob', 'sally', 'frank']`	property values in a predefined set
`sw`	`GET /AssetAccounts?filter=Name sw 'Sam'`	(v4 API only) starts with (for case insensitive searches use `isw`)
`ew`	`GET /AssetAccounts?filter=Name ew 'Smith'`	(v4 API only) ends with (for case insensitive searches use `iew`)

When using the `filter` parameter, you can use parenthesis () to group logical expressions. For example, `GET/Users?filter=(FirstName eq 'Sam' and LastName eq 'Smith') and not Disabled`

When using the `filter` parameter, use the backward slash character (\) to escape quotes in strings. For example: `Get/Users?filter=UserName contains '\''`

Using Safeguard PowerShell

PowerShell is a task-based command-line shell and scripting language used to automate tasks that manage operating systems and processes. The SPP Powershell module and scripting resources can be found on GitHub here: OneIdentity/safeguard-ps.

Installation

The SPP Powershell module is published to the PowerShell Gallery to make it easy to install using the built-in `Import-Module` cmdlet. Use the `Update-Module` cmdlet to get the latest functionality.

By default, Powershell modules are installed for all users. You need to be running Powershell as an Administrator to install for all users.

```
> Install-Module safeguard-ps
```

Or, you can install the modules just for you using the `-Scope` parameter which will never require administrator permission:

```
> Install-Module safeguard-ps -Scope CurrentUser
```

Using the virtual appliance and web management console

Before you start: platforms and resources

When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. See One Identity's Product Support Policies for more information on environment virtualization.

You must license the VM with a Microsoft Windows license. Specific questions about licensing should be directed to your Sales Representative.

Platforms and versions follow.

- You must license the VM with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative.
- Supported hypervisors:
  - Microsoft Hyper-V (VHDX) version 8 or higher
  - VMware vSphere with vSphere Hypervisor (ESXi) versions 6.5 or higher
  - VMware Workstation version 13 or higher
- Minimum resources: 4 CPUs, 10GB RAM, and a 500GB disk. The virtual appliances default deploy does not provide adequate resources. Ensure these minimum resources are met.

Available wizards

The Appliance Administrator responsible for racking and initial configuration of the appliance can create the virtual appliance, launch the Safeguard web management console, and select one of the following wizards.

- **Initial Setup**: Used to set up the virtual appliance for the first time including naming, OS licensing, and networking. For more information, see Setting up the virtual appliance on page 52.

- **Setup**: After the first setup, SPP updates and networking changes can be made via the web management console by clicking **Setup**.
- **Support Kiosk**: The **Support Kiosk** is used to diagnose and resolve issues with Safeguard for Privileged Passwords. Any user able to access the kiosk can perform low-risk support operations including appliance restart or shutdown and support bundle creation. In order to reset the admin password, the user must obtain a challenge response token from One Identity support. For more information, see Support Kiosk.

Security

CAUTION: To maximize security in the absence of a hardened appliance, restrict the access to the Safeguard virtual disks, the web management console, and the MGMT interface to as few users as possible. The Management web kiosk gives access to functions without authentication, such as pulling a support bundle and rebooting the appliance.

Security recommendations follow.

- X0 hosts the public API and is network adapter 1 in the virtual machine settings. Connect this to your internal network.
- MGMT hosts the web management console and is network adapter 2 in the virtual machine settings. This interface always has the IP address of 192.168.1.105. Connect this to a private, restricted network accessible to administrators only, or disconnect it from the network to restrict unauthenticated actions such as rebooting or shutting down the appliance. The web management console is also available via the VMware console.

Once setup is completed, you can verify which of your NICs is MGMT and X0 by referring to the MAC address information found in **Support Kiosk** > **Appliance Information** > **Networking** for X0 and MGMT. For more information, see Support Kiosk.

Backups: virtual appliance and hardware appliance

To protect the security posture of the Safeguard hardware appliance, Safeguard hardware appliances cannot be clustered with Safeguard virtual appliances. Backups taken from a hardware appliance cannot be restored on virtual appliances and backups taken from a virtual appliance cannot be restored on a hardware appliance.

For more information, see Virtual appliance backup and recovery.

Upload and download

There is a web management console running on 192.168.1.105. When you connect to the virtual appliance via the virtual display, the web management console is displayed automatically; however, upload and download functionality are disabled when connected this way.

You may choose to configure the networking of your virtual machine infrastructure to enable you to proxy to https://192.168.1.105 from your desktop. Connecting in this way will enable you to upload and download from the web management console.

> **CAUTION: Cloning and snapshotting are not supported and should not be used. Instead of cloning, deploy a new VM and perform Initial Setup. Instead of snapshotting, take a backup of the virtual appliance. Only the SPP backup and recovery functionality is supported (Virtual appliance backup and recovery).**

Migrating the VM

VMware VMotion can be used for live migration of a virtual machine from one physical server to another.

Setting up the virtual appliance

The Appliance Administrator uses the initial setup wizard to give the virtual appliance a unique identity, license the underlying operating system, and configure the network. The initial setup wizard only needs to be run one time after the virtual appliance is first deployed, but you may run it again in the future. It will not modify the appliance identity if run in the future.

Once set up, the Appliance Administrator can change the appliance name, license, and networking information, but not the appliance identity (`ApplianceID`). The appliance must have a unique identity.

The steps for the Appliance Administrator to initially set up the virtual appliance follow.

Step 1: Make adequate resources available

The virtual appliances default deploy does not provide adequate resources. The minimum resources required are: 4 CPUs, 10GB RAM, and a 500GB disk. Without adequate disk space, the patch will fail and you will need to expand disk space then re-upload the patch.

Step 2: Deploy the VM

Deploy the virtual machine (VM) to your virtual infrastructure. The virtual appliance is in the **InitialSetupRequired** state.

Hyper-V zip file import and set up

If you are using Hyper-V, you will need the Safeguard Hyper-V zip file distributed by One Identity to setup the virtual appliance. Follow these steps to unzip the file and import:

1. Unzip the `Safeguard-hyperv-prod...` zip file.
2. From Hyper-V, click **Options**.

3. Select **Action**, **Import Virtual Machine**.
4. On the **Locate Folder** tab, navigate to specify the folder containing the virtual machine to import then click **Select Folder**.
5. On the **Locate Folder** tab, click **Next**.
6. On the **Select Virtual Machine** tab, select `Safeguard-hyperv-prod....`
7. Click **Next**.
8. On the **Choose Import Type** tab, select **Copy the virtual machine (create a new unique ID)**.
9. Click **Next**.
10. On the **Choose Destination** tab, add the locations for the **Virtual machine configuration folder**, **Checkpoint store**, and **Smart Paging folder**.
11. Click **Next**.
12. On the Choose Storage Folders tab, identify **Where do you want to store the imported virtual hard disks for this virtual machine?**.
13. Click **Next**.
14. Review the **Summary** tab, then click **Finish**.
15. In the **Settings**, **Add Hardware**, connect to Safeguard's MGMT and X0 network adapter.
16. Right-click on the `Safeguard-hyperv-prod...` and click **Connect...** to complete the configuration and connect.

Step 3: Initial access

Initiate access using one of these methods:

- Via a virtual display: Connect to the virtual display of the virtual machine. You will not be offered the opportunity to apply a patch with this access method. Upload and download are not available from the virtual display. Continue to step 3. If you are using Hyper-V, make sure that Enhanced Session Mode is disabled for the display. See your Hyper-V documentation for details.
- Via a browser: Configure the networking of your virtual infrastructure to proxy https://192.168.1.105 on the virtual appliance to an address accessible from your workstation then open a browser to that address. For instructions on how to do this, consult the documentation of your virtual infrastructure (for example, VMWare). You will be offered the opportunity to apply a patch with this access method. Upload and download are available from the browser. Continue to step 3.

  > IMPORTANT: After importing the OVA and before powering it on, check the VM to make sure it doesn't have a USB controller. If there is a USB controller, remove it.

Step 4: Complete initial setup

Click **Begin Initial Setup**. Once this step is complete, the appliance resumes in the **Online** state.

Step 5: Log in and configure Safeguard for Privileged Passwords

1. If you are applying a patch, check your resources and expand the disk space, if necessary. The minimum resources are: 4 CPUs, 10GB RAM, and a 500GB disk.
2. To log in, enter the following default credentials for the Bootstrap Administrator then click **Log in**.
   - User Name: admin
   - Password: Admin123
3. If you are using a browser connected via https://192.168.1.105, the **Initial Setup** pane identifies the current Safeguard version and offers the opportunity to apply a patch. Click **Upload Patch** to upload the patch to the current Safeguard version or click **Skip**. (This is not available when using the Safeguard Virtual Kiosk virtual display.)
4. In the web management console on the **Initial Setup** pane, enter the following.
   a. **Appliance Name**: Enter the name of the virtual appliance.
   b. **Host DNS Suffix**: Enter the host DNS suffix name.
   c. **Windows Licensing**: Select one of the following options:
      - **Use KMS Server**: If you leave this field blank, Safeguard will use DNS to locate the KMS Server automatically. For the KMS Server to be found, you will need to have defined the domain name in the DNS Suffixes.

        If KMS is not registered with DNS, enter the network IP address of your KMS server.
      - **Use Product Key**: If selected, your appliance will need to be connected to the internet for the necessary verification to add your organization's Microsoft activation key.

   d. **NTP**: Complete the Network Time Protocol (NTP) configuration.
      - Select **Enable NTP** to enable the protocol.
      - Identify the **Primary NTP Server** IP address and, optionally, the **Secondary NTP Server** IP address.

   e. **Network (X0)**: For the X0 (public) interface, enter the IPv4 and/or IPv6 information, and **DNS Servers** information. Directory or network scans are supported for IPv4 but not IPv6.
5. Click **Save**. The virtual appliance displays progress information as it configures

Safeguard, the network adapter(s), and the operating system licensing.

6. When you see the message `Maintenance is complete`, click **Continue**.

Step 6: Access the web client

You can go to the virtual appliance's IP address for the X0 (public) interface from your browser.

Step 7: Change the Bootstrap Administrator's password

For security reasons, change the password on the Bootstrap Administrator User. For more information, see Setting a local user's password.For details, see the *Safeguard for Privileged Passwords Administration Guide*, Setting a local user's password.

Step 8. After clustering, change the trusted servers, CORS, and redirects setting

As a best practice, after you have created your Safeguard for Privileged Passwords cluster (or if just using a single VM), change the Trusted Servers, CORS and Redirects setting to the empty string or a list of values to integration applications you wish to allow. For more details, see the *Safeguard for Privileged Passwords Administration Guide*, Trusted Servers, CORS and Redirects.

View or change the virtual appliance setup

You can view or change the virtual appliance setup.

- From the web management console, click **Home** to see the virtual appliance name, licensing, and networking information.
- After the first setup, SPP updates and networking changes can be made via the web management console by clicking **Setup**.

Virtual appliance backup and recovery

Use the following information to back up and recover a SPP virtual appliance. Factory reset is not an option for virtual appliances. To factory reset a virtual appliance, just redeploy the appliance.

Backing up the virtual appliance

To ensure security of the hardware appliance, backups taken from a virtual appliance cannot be restored on a hardware appliance.

For more information, see Backup and Retention.Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Recovery of the virtual appliance

A SPP virtual appliance is reset by using the following recovery steps.

On-prem virtual appliance (for example, Hyper-V or VMware)

1. Redeploy the virtual appliance and run **Initial Setup**. For more information, see Setting up the virtual appliance.Setting up the virtual appliance in the *Safeguard for Privileged Passwords Administration Guide*.
2. Restore the backup. For more information, see Backup and Retention.Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Cloud virtual appliance (for example, AWS or Azure)

1. Redeploy using the deployment steps:
    - AWS: For more information, see AWS deployment.
    - Azure: For more information, see Azure deployment.
    - OCI: For more information, see OCI deployment.

Support Kiosk

An Appliance Administrator triaging a Hyper-V or VMware virtual appliance that has lost connectivity or is otherwise impaired can use the Support Kiosk even when the virtual appliance is in quarantine. For more information, see What do I do when an appliance goes into quarantine.What do I do when an appliance goes into quarantine in the *Safeguard for Privileged Passwords Administration Guide*.

It is recommended that terminal settings be 90 x 45 or larger. Smaller settings may result in a error like: `Screen dimension to small`.

When using the Windows Kiosk it is not possible to copy and paste. In Hyper-V it is possible to automate typing text from the keyboard, and using full ESX it may be possible to emulate keypresses via the API call `PutUsbScanCodes()`.

1. On the web management console, click **Support Kiosk**.
2. Select any of the following activities:
   - **Appliance Information**

     This is read-only. You can re-run setup to change networking information.
   - **Backups**

     Allows you to download or copy existing backups from quarantined appliances, so long as the appliance is not rebooted.

     a. In order to gain access to any previously generated backups, perform the challenge response process.

     b. Once the challenge response process is successful, click **Authorize Backup Downloads**.

     c. The **Backups** page will display the backup as well as any previously authorized backups. You will only have 24 hours after the successful authorization to access the backups. The following options are available once a backup has been generated:

        - **Delete Authorization**: Click this link to delete the authorization granted by the challenge response process. Once deleted, you will be unable to access the backups page until a new challenge response has been successfully completed.
        - (**Download**): Click this button to download the backup.
        - (**Copy to Share**): Click this button to copy the backup to a share. You must provide the UNC path and login credentials.
   - **Power Options**
     You can reboot or shutdown the virtual appliance.

     a. Enter the reason you want to reboot or shutdown the virtual appliance.

     b. Click **Reboot** or **Shutdown**.
   - **Admin Password Reset**

     The Bootstrap Administrator is a built-in account to get the appliance running for the first time. The default credentials (admin/Admin123) should be changed once Safeguard is configured. If you lose the password, you can reset it to the default using the challenge response process below.

     Challenge response process

     a. In **Full Name or Email**, enter your name or email to receive the challenge question.

     b. Click **Get Challenge**.

     c. To get the challenge response, perform one of the following (see the illustration that follows).

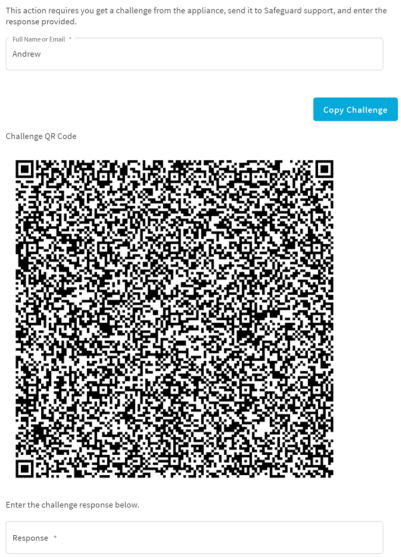
        - Click **Copy Challenge**. The challenge is copied to the clipbord. Send that challenge to Safeguard support. Support will send back a

challenge response that is good for 48 hours.

- Screenshot the QR code and send it to Support. Support will send back a challenge response that is good for 48 hours.

  IMPORTANT: Do not reboot the machine during the challenge response process.

- Use a QR code reader on your phone to get the challenge response.



d. After the response is accepted, click **Reset Password**. Once the operation has completed, the password for the admin account will be defaulted back to **Admin123**.

- **Support Bundle**
  A support bundle includes system and configuration information sent to One Identity Support to analyze and diagnose issues. You can download a support bundle or save the bundle to a Windows share location which you have already set up. To generate a support bundle:

  1. Select **Include Event Logs** if you want to include operating system events. Unless requested by support, it is recommended to leave this unchecked because it takes much longer to generate the support bundle.
  2. Create the support bundle using one of these methods:
     - If you are connected via the browser not the display, you can click **Download**, navigate to the location for the download, and click **OK**.
     - To copy the bundle to the share:
       1. Enter the **UNC Path**, **Username**, and **Password**.
       2. Select **Include Event Logs**, if appropriate.

3. Click **Copy To Share**. A progress bar displays. The operation is complete when you see `The bundle was successfully copied to the share.`

- **Diagnostic package**

  Appliance Administrators can execute a trusted, secure appliance diagnostics package to help solve issues with configuration, synchronization, and clustering, as well as other other internal challenges. The appliance diagnostics package is available from the web Support Kiosk, not the Serial Kiosk (Recovery Kiosk). The appliance diagnostics package can be used even when the appliance is in quarantine. To protect against external threats, Safeguard rejects illegitimate appliance diagnostics packages. The manifest file in the appliance diagnostics package lists criteria that may include the minimum Safeguard version, appliance ID, and expiration time-stamp UTC. New product code and database changes are not included in an appliance diagnostics package.

  a. To load for the first time, click **Upload**, select the file that has an .sgd extension, then click **Open**.

     - If the upload criteria is not met, the appliance diagnostics package is not uploaded and a message like the following displays: `The minimum Safeguard version needed to run this diagnostic package is <version>.`
     - If the upload is successful, the **Diagnostic Package Information** displays with a **Status** of **Staged**. Select **Execute** and wait until the **Status** changes to **Completed**.

  b. Once uploaded, you can:

     - Select **Download Log** to save the log file. Audit log entries are available through the Activity Center during and after execution and are part of the appliance history.
     - If the **Expiration Date** has not passed, you can select **Execute** to execute the appliance diagnostics package again.
     - Select **Delete** to delete the appliance diagnostics package, the associated log file, and stop any appliance diagnostics package that is running. Before uploading a different appliance diagnostics package, you must delete the current one because there can be only one appliance diagnostics package per appliance.

Cloud deployment considerations

SPP can be run from the cloud.

Before you start: platforms and resources

When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. See One Identity's Product Support Policies for more information on environment virtualization.

Platforms that have been tested with the cloud deployments follow.

- AWS Virtual Machine (VM): For more information, see AWS deployment.
- Azure Virtual Machine (VM): For more information, see Azure deployment.
- Oracle Cloud Infrastructure (OCI): For more information, see OCI deployment.

For these deployments, the minimum resources used in test are 4 CPUs, 10GB RAM, and a 60GB disk. Choose the appropriate machine and configuration template. For example, when you click **Create** in the Azure Marketplace, default profiles display. You can click **Change size** to choose a different template. Whereas in OCI, select a supported shape to allocate the appropriate resources for your instance.

Restricting access to the web management kiosk for cloud deployments

The web management kiosk runs on port 9337 in AWS, OCI, and Azure and is intended for diagnostics and troubleshooting by Appliance Administrators.

CAUTION: The Management web kiosk is available via HTTPS port 9337 for cloud platforms (including AWS, OCI, and Azure). The Management web kiosk gives access to functions without authentication, such as pulling a support bundle or rebooting the appliance. In AWS and OCI, all ports are denied unless explicitly allowed. To deny access to port 9337, the port should be left out of the firewall rules. If the port is used, firewall rules should allow access to targeted users.

Azure: Block port 9337

Use the following steps to block access to port 9337 in Azure.

1. Navigate to the virtual machine running SPP.
2. In the left hand navigation menu select **Networking**.
3. Click **Add inbound port rule**.
4. Configure the inbound security rule as follows:
   Source: Any
   Source port ranges: *
   Destination: Any
   Destination port ranges: 9337
   Protocol: Any
   Action: Deny
   Priority: 100 (use the lowest priority for this rule)
   Name: DenyPort9337
5. Click **Add**.

AWS: Block port 9337

Use the following steps to block access to port 9337 in AWS.

1. From the EC2 Dashboard, navigate to the EC2 Instance running SPP.
2. Select the instance.
3. In the **Description** tab, locate the **Security groups** field then click the name of the security group.
4. Select the **Inbound** tab.
5. Click **Edit**.
6. Remove any existing rules and add the following rules:
   - Type: Custom UDP Rule
     Protocol: UDP
     Port Range: 655
     Source: Anywhere
     Description: Cluster VPN
   - Type: HTTPS
     Protocol: TCP
     Port range: 443
     Source: Anywhere
     Description: Web API
   - Type: Custom TCP Rule
     Protocol: TCP
     Port Range: 8649
     Source: Anywhere
     Description: SPS Cluster
7. Click **Save**.

OCI: Block port 9337

Use the following steps to block access to port 9337 in OCI.

1. Navigate to the Virtual Cloud Network assigned to the instance running SPP.
2. Navigate to the **Subnet** assigned to the instance.
3. Open the **Security List** for the subnet.
4. Ensure no ingress rules allow for traffic from any source (with any IP Protocol) to destination port 9337. Review the ingress rules carefully as they may apply to a range of destination ports instead of explicitly listing port 9337.

AWS deployment

IMPORTANT: Before deploying, make sure you have read Cloud deployment considerations

SPP (SPP) can be run in the cloud using Amazon Web Services (AWS).

To deploy the Amazon Machine Image (AMI) of SPP from AWS, visit the AWS marketplace listing for SPP (here) and follow the Deployment steps.

Disk size considerations

CAUTION: Before making any changes to the disk size, shut down the VM (stopped and deallocated).

SPP deploys with a minimal OS disk size. You should increase the size of the OS disk based on your estimated usage and budget. SPP on hardware comes with 1TB of disk. You can use more or less than this depending on how many assets, accounts, and daily users you expect to have. 500GB is a minimal production disk size and 2TB is the maximum.

Disk size can be handled through Amazon Elastic Compute Cloud (Amazon EC2). For more information, see Getting Started with Amazon EC2. When you start up the VM, SPP automatically resizes the OS disk volume to use the available space.

AWS security considerations

Running SPP in AWS comes with some security considerations that do not apply to the hardware appliance. We recommend:

- Do not give Safeguard a public IP address.
- Use the AWS key vault to encrypt the disk.
- Limit access within AWS to the Safeguard virtual machine. SPP in AWS cannot protect against rogue Administrators in the same way the hardware appliance can.

Static IP address required

Configure the SPP VM with a static IP address in AWS. In AWS, the IP address must not change after the VM is deployed. If you need to change the IP address, take a backup, deploy again, and restore the backup. You can script the VM deploy to pick up an existing virtual NIC with the IP address configuration. For details, see the Amazon Virtual Private Cloud (VPC) documentation.

Deployment steps

AWS automatically licenses the operating system during the deployment with an AWS KMS.

Larger deployments warrant larger sizing choices. SPP hardware appliances have 32GB of RAM and 4 processors with at least 1TB of disk space.

AWS Marketplace steps

1. Go to the AWS marketplace listing for SPP (here).
2. On the One Identity Safeguard for Privileged Passwords page, click **Continue to Subscribe**.
3. Advance through the resource creation screens to configure your instance. In addition to the Disk size considerations, AWS security considerations, and Static IP address required; One Identity recommends you select the **m4.2xlarge** instance type.
4. Once you have finished configuring the instance, select to launch the instance.

   NOTE: The instance launch process may take a while to complete.
5. Once the instance has finished launching, log into the web client using your static IP address. You will need to use the default username (**`admin`**) and password (**`<instance id>`**). You should change the admin password immediately. For more information, see Setting a local user's password on page 548.For details, see *Setting a local user's password* in the *Safeguard for Privileged Passwords Administration Guide*.

   NOTE: The password is unique for each deployment and the initial password will always be the instance ID of the deployed safeguard server.

View or change the cloud virtual appliance setup

You can view or change the virtual appliance setup.

You can use the SPP web management kiosk on port **9337** for diagnostics and troubleshooting.

You can also check the system logs via AWS:

1. To view the system log from AWS, select **Actions**, then **Instance Settings**, and then **Get System Log**.
2. Log in via `https://<your IP>:9337`

To patch to a new version, use the API.

Azure deployment

IMPORTANT: Before deploying, make sure you have read Cloud deployment considerations

SPP (SPP) can be run in the cloud using Azure. A version of SPP is available in the Azure Marketplace and an Azure Virtual Machine (VM) is required. See Windows virtual machines in Azure for details of setting up your VM.

When using Azure, SPP is available on HTTPS X0. The Azure deployment does not use the MGMT service. The Recovery (Serial) Kiosk is used to view appliance information, Administrator password reset, power restart or shut down, and generating a support bundle. For more information, see Recovery Kiosk (Serial Kiosk).*Recovery Kiosk (Serial Kiosk)* in the *Safeguard for Privileged Passwords Administration Guide*.

Disk size considerations

SPP deploys with a minimal OS disk size. You should increase the size of the OS disk based on your estimated usage and budget. SPP on hardware comes with 1TB of disk. You can use more or less than this depending on how many assets, accounts, and daily users you expect to have. 500GB is a minimal production disk size and 2TB is the maximum.

1. Deploy SPP.
2. Verify you can log in.
3. Shut down the VM (stopped and deallocated).
4. Follow Microsoft's guidance for increasing the disk size: How to expand the OS drive of a virtual machine.

When you start up the VM, SPP automatically resizes the OS disk volume to use the available space.

Azure security considerations

Running SPP in Azure comes with some security considerations that do not apply to the hardware appliance. We recommend:

- Do not give Safeguard a public IP address.
- Use the Azure key vault to encrypt the disk.
- Limit access within Azure to the Safeguard virtual machine. SPP in Azure cannot protect against rogue Administrators in the same way the hardware appliance can.

Static IP address recommended

Configure the SPP VM with a static IP address in Azure. In Azure, the IP address must not change after the VM is deployed. If you need to change the IP address, take a backup, deploy again, and restore the backup. You can script the VM deploy to pick up an existing virtual NIC with the IP address configuration. For details, see Microsoft's Virtual Network documentation.

Deployment steps

SPP is deployed from the Azure Marketplace. Azure automatically licenses the operating system during the deployment with an Azure KMS.

The Azure base image includes the required configuration necessary to deploy into Azure following Microsoft's guidance, Prepare a Windows VHD or VHDX to upload to Azure.

1. Log into the Azure portal.
2. Under **Azure services**, click **Create a resource**.
3. Search for "One Identity Safeguard for Privileged Passwords" and click the tile.
4. On the One Identity Safeguard for Privileged Passwords screen, click **Create**.
5. Advance through the resource creation screens. Considerations follow:
   - For small deployments, it is recommended to choose at least VM size Standard D2s v3. Larger deployments warrant larger sizing choices. Safeguard hardware appliances have 32GB of RAM and 4 processors with at least 1 TB of disk space.
   - You must set an administrator user name and password as part of the image creation, however, SPP will disable this account during initial setup.
   - Set public inbound ports to **None**.
   - Choose your Windows licensing option.
   - Make sure to enable boot diagnostics and the serial kiosk. The Azure Serial console will be used to provide access to the Safeguard Recovery Kiosk.
6. Once you are finished configuring the VM, click **Create**. Azure will deploy the SPP virtual machine.
7. When the virtual machine deployment is finished, SPP will automatically start initializing and configuring itself for the first use. This usually takes between 5-30 minutes, depending on the VM sizing. During initialization, Safeguard will enable the firewall and disable remote access to the VM. You can monitor the progress of initialization from the Azure Serial console. While the initialization is running, do not log in to the VM or power off or restart the VM.
8. When initialization is complete, you will see the Safeguard Recovery (Serial) Kiosk on the Azure Serial console screen.
9. Log in to the appliance via the web using the default username and password admin / Admin123. You should change the admin password immediately. For more information, see Setting a local user's password on page 548.For details, see *Setting a local user's password* in the *Safeguard for Privileged Passwords Administration Guide*.
10. After clustering, change the trusted servers, CORS and redirects setting.

    As a best practice, after you have created your Safeguard for Privileged Passwords cluster (or if just using a single VM), change the Trusted Servers, CORS and Redirects setting to the empty string or a list of values to integration applications you wish to allow. For more information, see *Trusted Servers, CORS and Redirects* in the *Safeguard for Privileged Passwords Administration Guide*.

View or change the cloud virtual appliance setup

You can view or change the virtual appliance setup.

The Administrator uses the Recovery Kiosk (Serial Kiosk) to perform the following.

- Get appliance information
- Reset the Administrator password
- Restart or shut down the virtual appliance
- Generate a support bundle
- Resolve a quarantine (for more information, see What do I do when an appliance goes into quarantineWhat do I do when an appliance goes into quarantine in the *Safeguard for Privileged Passwords Administration Guide*).

For more information, see Recovery Kiosk (Serial Kiosk).Recovery Kiosk (Serial Kiosk) in the *Safeguard for Privileged Passwords Administration Guide*.

To patch to a new version, use the API.

OCI deployment

IMPORTANT: Before deploying, make sure you have read Cloud deployment considerations

SPP ([Official abbreviation of the product name]) can be run in the cloud using Oracle Cloud Infrastructure (OCI).

Disk size considerations

CAUTION: Before making any changes to the disk size, shut down the VM (stopped and deallocated).

SPP deploys with a minimal OS disk size. You should increase the size of the OS disk based on your estimated usage and budget. SPP on hardware comes with 1TB of disk. You can use more or less than this depending on how many assets, accounts, and daily users you expect to have. 500GB is a minimal production disk size and 2TB is the maximum.

1. Deploy SPP.
2. Verify you can log in.
3. Shut down the VM (stopped and deallocated).
4. Follow Oracle's guidance for increasing the boot volume (Resizing a Volume).

NOTE: When you start up the VM, SPP automatically resizes the OS disk volume to use the available space.

OCI security considerations

Running SPP in OCI comes with some security considerations that do not apply to the hardware appliance. We recommend:

- Do not give Safeguard a public IP address.
- Use the OCI key vault to encrypt the disk.
- Limit access within OCI to the Safeguard virtual machine. SPP in OCI cannot protect against rogue Administrators in the same way the hardware appliance can.

Deployment steps

SPP is deployed using a custom image which you can download from the One Identity Support Portal. OCI automatically licenses the operating system during the deployment with an OCI KMS.

Larger deployments warrant larger sizing choices. SPP hardware appliances have 32GB of RAM and 4 processors with at least 1TB of disk space.

To deploy [Official abbreviation of the product name]

1. Go to the One Identity Support Portal for SPP.
2. On the One Identity Safeguard for Privileged Passwords page, on the side panel, under **Self Service Tools**, click **Software Downloads**.
3. To download the OCI image, click ⭳ next to the image.
4. Once you have downloaded the image, import it.

   For instructions, see Importing Custom Windows Images.
5. Once the instance has finished launching, log into the web client using your static IP address. You will need to use the default user name (**`admin`**) and password (**`<instance id>`**). You should change the admin password immediately. For more information, see Setting a local user's password.For details, see the *Safeguard for Privileged Passwords Administration Guide*, Setting a local user's password.

   > NOTE: The password is unique for each deployment and the initial password will always be the instance ID of the deployed safeguard server.

View or change the cloud virtual appliance setup

You can view or change the virtual appliance setup.

You can use the SPP web management kiosk on port **`9337`** for diagnostics and troubleshooting. In order to access the kiosk on an OCI appliance, an administrator must create a policy to allow cloud shell access. You can the access the kiosk by connecting to the Cloud Shell. Once connected, to display the kiosk, press **Ctrl+r**. For more information on Cloud Shell, see Cloud Shell in the *Oracle Cloud Infrastructure Documentation*.

You can check the system logs on the **Logging Audit** page in OCI.

To patch to a new version, use the API.

Virtual appliance backup and recovery

Use the following information to back up and recover a SPP virtual appliance. Factory reset is not an option for virtual appliances. To factory reset a virtual appliance, just redeploy the appliance.

Backing up the virtual appliance

To ensure security of the hardware appliance, backups taken from a virtual appliance cannot be restored on a hardware appliance.

For more information, see Backup and Retention.Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Recovery of the virtual appliance

A SPP virtual appliance is reset by using the following recovery steps.

On-prem virtual appliance (for example, Hyper-V or VMware)

1. Redeploy the virtual appliance and run **Initial Setup**. For more information, see Setting up the virtual appliance.Setting up the virtual appliance in the *Safeguard for Privileged Passwords Administration Guide*.
2. Restore the backup. For more information, see Backup and Retention.Backup and Retention settings in the *Safeguard for Privileged Passwords Administration Guide*.

Cloud virtual appliance (for example, AWS or Azure)

1. Redeploy using the deployment steps:
    - AWS: For more information, see AWS deployment.
    - Azure: For more information, see Azure deployment.
    - OCI: For more information, see OCI deployment.

Setting up Safeguard for Privileged Passwords for the first time

Before One Identity Safeguard for Privileged Passwords can manage your privileged account passwords and privileged sessions, you must first add all the objects you need to write access request policies, such as users, accounts, and assets. By following these procedures, you will set up a hierarchy of administrators that ensures your company follows role-based access control. For more information, see Administrator permissions on page 604.

The setup steps in this section assume you have completed the appliance initial installation and configuration steps in the *One Identity Safeguard for Privileged Passwords Appliance Setup Guide*.

Before SPP can reset local account passwords on Windows systems, you must change the local security policy to disable **User Account Control: Run all administrators in Admin Approval Mode**. For more information, see Change password or SSH key fails on page 638.

Step 1: Create the Authorizer Administrator

Step 2: Authorizer Administrator creates administrators

Step 3: Appliance Administrator configures the appliance

Step 4: User Administrator adds users

Step 5: Asset Administrator adds managed systems

Step 6: Security Policy Administrator adds access request policies

Step 1: Create the Authorizer Administrator

1. Log in using the Bootstrap Administrator account. (The password was changed from the default when you created the appliance using the instructions in the *Safeguard for Privileged Passwords Appliance Setup Guide*.)

2. Create the Authorizer Administrator, which is a user who can authorize other administrators. Give the user **Authorizer** permissions so the user can grant permissions to other users and change their own permissions. For more information, see Adding a user on page 541.
3. Log out as the Bootstrap Administrator.
4. Log in as the Authorizer Administrator.
5. Disable the Bootstrap Administrator.

Step 2: Authorizer Administrator creates administrators

Add the user administrator permissions. A user can have more than one set of permissions. For a list of permissions granted to the different SPP administrators, see Administrator permissions.

1. Make sure you have logged in using the Authorizer Administrator account.
2. Customize the Local Password Rule. (Navigate to **Appliance Management** > **Safeguard Access** > **Local Password Rule**.)
3. Add users for the following administrator permissions (Adding a user):
   a. User Administrator
   b. Help Desk Administrator
   c. Appliance Administrator
   d. Operations Administrator
   e. Auditor
   f. Asset Administrator
   g. Security Policy Administrator

Step 3: Appliance Administrator configures the appliance

1. Log in using the Appliance Administrator account.
2. Navigate to **Appliance Management** > **Appliance** > **Networking** and set the following:
   a. IP Address
   b. Netmask

c. Default Gateway
d. DNS Servers
e. DNS Suffixes

For more information, see Networking on page 141.

3. Ensure the access request as well as password and SSH key management features are enabled. For more information, see Global Services.
4. (Optional) Enable or disable Application to Application (A2) and audit data sharing with Safeguard for Privileged Sessions. For more information, see Global Services.
5. Configure the External Integration that apply:
   a. Email: Configure the SMTP server to be used for email notifications. SPP provides default email templates for most events, which can be customized. For more information, see Email on page 218.
   b. Identity and Authentication: Configure directory services such as Active Directory and LDAP servers to be used as identity and authentication providers for SPP users. Configure SPP as a relying party that uses SAML 2.0 to integrate with external federation services to authenticate users. Create a RADIUS server to be used as a primary or secondary authentication provider. For more information, see Identity and Authentication on page 254.
   c. SNMP: Configure SNMP subscriptions for sending SNMP traps to your SNMP console when certain events occur. For more information, see SNMP on page 226.
   d. Starling: Join SPP to Starling to take advantage of other Starling services. For more information, see Starling on page 229.
   e. Syslog: Configure the syslog servers where event notifications are to be sent. For more information, see Syslog on page 232.
   f. Ticket Systems: Add external ticketing tracking system or track tickets not tied to an external ticketing system. For more information, see Ticket systems.

Step 4: User Administrator adds users

1. Log in using the User Administrator account.
2. Add users who can log in to Safeguard for Privileged Passwords (Adding a user).
3. Grant Help Desk Administrator permissions to one or more users.

Step 5: Asset Administrator adds managed systems

1. Log in using the Asset Administrator account.
2. Add partitions and, optionally, delegate partition ownership to other users (Adding a partition).
3. (Optional) Set the following Password Profiles (or edit the default rules and settings defined when the partition was added):
   - Account Password Rules
   - Change Password
   - Check Password
   - Password sync groups
4. (Optional) Set the following SSH Key Profiles:
   - Change SSH Key settings
   - Check SSH Key settings
   - Discover SSH Key settings
   - SSH Key Sync Groups settings
5. (Optional) Create profiles or edit the default profiles created (Creating a password profile).
6. Add assets to the appropriate partitions and profiles (Adding an asset).
7. Add accounts to control access to the assets (Adding an account).

TIP: Create asset and account discovery jobs to discover and, optionally, automatically add assets and accounts to Safeguard for Privileged Passwords. For more information, see Discovery on page 364.

Step 6: Security Policy Administrator adds access request policies

1. Log in using the Security Policy Administrator account.
2. Set Reasons.
3. Add user groups (Adding a user group).
4. Add local or directory users to local user groups (Adding users to a user group).
5. Add account groups (Adding an account group).
6. Add accounts to account groups (Adding one or more accounts to an account group).

7. Add entitlements (Adding an entitlement).
8. Add users or user groups to entitlements (Adding users or user groups to an entitlement).
9. Create access request policies (Adding an entitlement).

Using the web client

The web client uses a responsive user interface design to adapt to the user's device, from desktops to tablets or mobile phones. Only one user session will persist during a browser session. Any tabs opened after initial authentication will use the existing user session.

To log into the web client application

The following steps assume the One Identity Safeguard for Privileged Passwords Appliance has been configured and licensed. As a SPP user, if you get an `appliance is unlicensed` notification, contact your Appliance Administrator.

1. From your browser, enter the SPP URL with the IP address, such as `https://11.1.111.11`.
2. If a login notification displays, click **OK** to accept the notifications and restrictions stated.
3. On the user log in screen, enter your credentials and click **Log in**.

Updating your avatar photo

To change your photo in the web client, expand the **Username** drop-down in the upper right and select **My Settings**. On the **My Settings** page, select **My Account** and click the circle icon with the username. Select the image file (under 64 KiB), then click **Open**.

Using the left navigation menu

NOTE: Use the button on mobile devices to expand and collapse the navigation menu.

The pages available to you display on the left. Clicking one of the top level headings from the left navigation menu will expand the section to display the associated subpages. For example, clicking **User Management** will expand the navigation menu to show all pages associated with managing users that you have permission to access.

You can reduce the left menu using the button located at the bottom of the left navigation menu.

My Settings

From **My Settings**, you can set a variety of controls for using the web client. The settings you see are based on your role and permissions.

Go to My Settings

In the upper right corner, next to your user name, click ▼ then **My Settings** to proceed.

On the **My Settings** dialog, the tabs available are based on your role and permissions.

Using the ⚙ General tab

- Language drop-down: Use this drop-down to change the site language. By default, this is set to **Browser Language (Auto Detect)**.
- **About Safeguard**: The **Appliance Version** displays.

Using the My Account tab

- **Contact Information:** Click ✎ **Edit** to change **Email**, **Work Phone**, or **Mobile Phone**. Click ✓ **Save** to save your changes or click ✕ **Cancel** to revert to the previous setting.
- **Location**: Select your time zone in the drop-down box. Changing your time zone may be prohibited based on your organization's security procedures. If available, choose to:
  - **Display times in local computer time**: This is the default. It is the time zone set on your local computer.
  - **Display times in my configured time zone**: This is the time zone that is set on this page.
- **Manage Email Notifications**: The **Manage Email Notifications** dialog displays the type of events for which you are receiving email notifications. You can define the types of events for which you want to receive notifications. By default, all events are selected. If the event is **Built In** to SPP, a ✓ displays. When there are multiple events, an **Events** link appears that leads to the **Subscriptions** dialog listing the **Name**, **Description**, and **Category** of the event.
  - Clear the check box for any events for which you do not want to receive an email notification.
  - To set all check boxes, select or clear the check box at the top of the list to the left of the header.

> NOTE: When there are no delegated owners assigned to a partition, email notifications related to partitions are sent to the Asset Administrator. However, when a delegated owner is specified to manage the assets and accounts in a partition, email notifications related to partitions are sent to the delegated owner, not to the

Asset Administrator.

- **Manage FIDO2 Keys** (Available if you are required to perform FIDO2 two-factor authentication.): If the FIDO2 feature is enabled, at least one FIDO2 key must be registered. When a key is added, the placeholder name is **Unnamed Key**. You can enter a meaningful name or later edit the name. It is recommended that all users have more than one key registered in case a key is lost or damaged. For existing keys, you will see the name and date each existing key was registered and last used.
  - To change a name, enter the new name, then click **Save**.
  - To remove a key, click **Remove** by the key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.
  - To add a key, click **Register New FIDO2 Key**.
    a. You will be asked to insert or connect to the new key.
    b. You will be prompted to reenter your primary credentials for verification.
    c. Tap or activate your new FIDO2 key that is being registered.
    d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name, then click **Save**.

    For more information, see Requiring user to log in using secondary authentication.
- **Change Password**: The password requirements are listed. Enter your **Current Password** and the **New Password** as directed. (Click **Display** or **Hide** to view or hide the password as it is entered.) Click **Save**.

Change password

You can change your password.

To change the password

1. In the upper right corner, next to your user name, click .
2. Click **My Settings**.
3. Open the **My Account** tab.
4. Click **Change Password**. The password requirements are listed.
5. Enter your **Current Password** and the **New Password** as directed. (Click **Display** or **Hide** to view or hide the password as it is entered.)
6. Click **Save** to save your new password.

FIDO2 keys

If the FIDO2 feature is enabled, at least one FIDO2 key must be registered. When a key is added, the placeholder name is **Unnamed Key**. You can enter a meaningful name or later edit the name. It is recommended that all users have more than one key registered in case a key is lost or damaged.

1. In the upper right corner, next to your user name, click .
2. Click **My Settings**.
3. Open the **My Account** tab.
4. Click **Manage FIDO2 Keys**. For existing keys, you will see the name and date each existing key was registered and last used.
5. Perform an action:
   - To change a name, enter the new name, then click **Save**.
   - To remove a key, click **Remove** by the key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.
   - To add a key, click **Register New FIDO2 Key**.
     a. You will be asked to insert or connect to the new key.
     b. You will be prompted to reenter your primary credentials for verification.
     c. Tap or activate your new FIDO2 key that is being registered.
     d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name, then click **Save**.

For more information, see Requiring secondary authentication log in.Requiring secondary authentication log in in the *Safeguard for Privileged Passwords Administration Guide*.

Application switcher

Accessible from the toolbar, the application switcher allows you to navigate between One Identity products related to SPP.

To use the application switcher

1. In the upper right corner, next to your user name, click the button to display the One Identity products available for access. Some products, such as Safeguard for Privileged Sessions, require they be linked before becoming available in the application switcher.
2. Click one of the listed products to open it in a new tab.

Log out

Always securely log out of the web client. Log events are created based on how the user logged out: `UserLoggedOut` or `InactiveUserLoggedOut`.

To log out

1. In the upper right corner, next to your user name, click ▼.
2. Click **Log Out** to securely exit the SPP web client.

Search box

The search box can be used to filter the data being displayed. When you enter a text string into the search box, the results include items that have a string attribute that contains the text that was entered. This same basic search functionality is also available for many of the detail panes and dialogs, allowing you to filter the data displayed in the associated pane or dialog.

When searching for objects in the object lists, an attribute search functionality is also available where you can filter the results, based on a specific attribute. That is, the search term matches if the specified attribute contains the text. To perform an attribute search, click the 🔍 icon to select the attribute to be searched.

Rules for using the search functionality:

- Search strings are not case-sensitive. Exception: the Approvals and Reviews searches are case sensitive.
- When you click on the search icon in the search bar you will see a drop down of available search attributes (columns) for the grid. This can be used in conjunction with the entered search strings.

  Some of the search attributes will also have an arrow to expand subsearches. These subsearches have pre-defined search strings.
- By default, results are displayed in alphabetical order.
- Wildcard searches are allowed.
- Try using quotes and omitting quotes. As you use the product, you will become familiar with the search requirements for the search fields you frequent. Safeguard may perform a general search (for example, omits quotes) or a literal search (for example, includes quotes). Example scenarios follow:
  - On **Appliance Management** > **Search**, search strings must be an exact match because a literal search is performed. Do not add quotes or underlines. For example, from the Settings pane, enter `password rule` to return **Safeguard Access** > **Local Password Rule**. If you enter **"password rule"** or **password_rule**, the following message is returned: `No matches found`.

    - On the Users pane search box, you can use quotes in an attribute search if there are spaces in the search name. For example, entering the following in the search box **Username: "ab misc2"** returns: `AB misc2`.
- When multiple search strings are included, all search criteria must be met in order for an object to be included in the results list. In the web client, if conflicting attributes are entered for the same search (for example, both true and false) then the results will expand to show all matches so long as they fit one of those attributes.
- When you combine a string search and an attribute search, the order they are entered into the search box matters. The attribute searches can be in any order, but the string search must come after the attribute searches.
- To search using dates and times in the web client, the following format is used: `YYYY-MM-DDThh:mm:ss`. For example, if you are searching for an entitlement that expires December 1, 2021 then you would use the following search: `ExpirationDate:2021-12-01`. To include a minimum and maximum value in a search, use `..` to separate two values. For example, if you are searching for an entitlement that expires between December 1, 2021 and December 3, 2021 then you would use the following search: `ExpirationDate:2021-12-01..2021-12-03`.

To search for objects or object details

1. Enter a text string in the **Search** box. As you type, the list displays items whose string attributes contain the text that was entered.

   Examples:

   - Enter **T** in the search box to search for items that contain the letter "T".
   - Enter **sse** to list all items that contain the string "sse," (such as "Asset").

   NOTE: The status bar along the bottom of the console shows the number of items returned.

2. To clear the search criteria, click the ✕ button in the search box.

   When you clear the search criteria, the original list of objects is displayed.

You can also Search by attribute.

Search by attribute

The attributes available for searching are dependent on the type of object being searched. The search drop-down menu lists the attributes that can be selected.

API attributes can be searched

The drop-down menu lists a limited number of attributes that can be searched; however, you can perform an attribute search using the English name of any attribute as it appears in the API (for example, searching on `Display Name` would be `DisplayName: <My Display Name>`). Nested attributes can be chained together using a period (`.`). To see a list of all the

attributes, see the API documentation. For more information about the API, see Using the API.

Entering the search string

1. Click the 🔍 icon and select the attribute to be searched.

   The selected attribute is added to the search box. For example, if you select **Last Name** then **LastName:** is added to the search box.

2. In the search box, enter the text string after the colon in the attribute label.

   You can specify multiple attributes, repeating these steps to add an additional attribute to the search box. Do not add punctuation marks, such as commas or colons, to separate the different attributes. When multiple attributes are included, all search criteria must be met in order for an object to be included in the results list. In the web client, if conflicting attributes are entered for the same search (for example, both true and false) then the results will expand to show all matches so long as they fit one of those attributes.

   As you type, the list displays items whose selected attributes contain the text that was entered.

   > NOTE: The status bar along the bottom of the console shows the number of items returned.

3. To clear the search criteria, click the ✕ button.

   When you clear the search criteria, the original list of objects are displayed.

Exporting data

Throughout the web client, when an **Export** button appears above a table it indicates that the data appearing in the table can be exported as either a JSON or CSV file.

To export data

1. Navigate to the page displaying the information to be exported. For example, if you want to export user information in order to see who can log into the product then you would navigate to the **Users** page.
2. (Optional) Apply filters or search criteria to the displayed data.
3. Click the **Export** button.
4. On the export dialog, select **CSV** or **JSON**. Different information may be available depending on your selection. For example, when the data covers an array of information then the CSV will only report the number of items in the array whereas the JSON will contain the full list. This can be seen when exporting Account Groups data; the CSV will show the number of accounts in a group, but the JSON will show all of the information for all the accounts in a group.

5. Click **Fields** to open the **Export Fields** dialog where you can select which fields to include in the report. The **Export Fields** dialog will be prepopulated with the selections made during the last export of data from the page.
6. Click **OK** to save your selection.
7. Click **Sort By** to open the **Export Sort Order** dialog where you can select the order in which to sort the previously selected fields. This allows you to organize the exported data according to your needs.
   - **Add Sort Order**: Use this button to add additional fields by which to sort the data.
   - **Clear All Sort Orders**: Use this button to clear all selected fields.
   - **Drag up or down to change the sort order**: When you have multiple sort orders, click and hold this icon with your cursor then drag the selected sort order to whichever spot in the list you want.
   - **Order By**: Use this drop-down to select a field by which to sort the data.

     Additional drop-downs are added using the **Add Sort Order** button. The **Order By** fields will be prepopulated with the selection(s) made during the last export of data from the page.
   - or **Change Sort Direction**: Clicking this button changes the sort direction for the field. For example, if you have selected FirstName in the **Order By** drop-down and as the sort direction, your exported data will order the results in alphabetical order based on FirstName.
   - : Clicking this button removes the associated **Order By** selection.
8. Click **OK** to save your selection.
9. Selecting the **Limit Results** check box displays the **Number of results to include** field which is used to limit the number of results that will be included in the exported file. The **Number of results to include** field will be prepopulated with the selection made during the last export of data from the page.
10. Click **Export**.

8

Home page

Click **Home** to go to the home page. The **Home** page can be tailored to your role by allowing you to show or hide many of the tiles that can be displayed. For example, the page displays tiles for **My Requests**, **Approvals**, and **Reviews**, where each tile contains the number of tasks and their status, such as **Available**, **Denied**, **Revoked**, or **Pending**, and also the number of tasks **Due Today**.

For some administrator users, additional tiles for **Appliance Resources**, **Cluster Status**, **Access Request Activity**, **Account Automation**, and **Running Tasks** can also be displayed.

All users can choose to read the **Message of the Day** that the Appliance Administrator sets. For more information, see Message of the Day.

To set the displayed tiles on your home page, click **Settings**. The opening side sheet allows you to toggle the display of any of the tiles available to your role.

For Requesters

All users of Safeguard for Privileged Passwords have the right to submit an access request, if they have been assigned to an entitlement. A requester user can hide all tiles on the home page except for the **My Requests** and **Most Recently Used Favorites**. To submit an access request, see the following for more information:

- Requesting a password release
- Requesting an SSH key release
- Requesting an API key release
- Requesting session access

After an access request has been submitted, the user can click the **My Requests** tile to view the requests awaiting action. For more information, see:

- Taking action on a password release request
- Taking action on an SSH key release request
- Taking action on an API key release request
- Taking action on a session request

The **Most Recently Used Favorites** tile shows a list of up to 5 of your most recently used favorite requests.

For Approvers

An approver can be added to an access request policy to approve or deny an access request made by another user. An approver can hide all tiles on the home page except for the **Approvals**, unless the user is also responsible for other roles. For more information on approving access requests, see:

- Approving a password release request
- Approving an SSH key release request
- Approving an API key release request
- Approving a session request

For Reviewers

A reviewer can be added to an access request policy to review completed access requests. A reviewer can hide all tiles on the home page except for the **Reviews**, unless the user is also responsible for other roles. For more information on reviewing access requests, see:

- Reviewing a completed password release request
- Reviewing a completed SSH key release request
- Reviewing a completed API key release request
- Reviewing a session request

My Requests

If you are a requester, click **My Requests** to make a request or see information about requests.

If **Show Account Availability** is enabled, you can identify if a privileged account is available or not. Accounts display a warning badge if in use by a request. An account's status is updated immediately after being changed in order to avoid overlapping account requests from multiple users. Hover over the badge to display `<X> of <X> accounts in use`. Showing account availability requires additional API queries that may impact performance. This toggle is set by the user, not an administrator. There is no global toggle.

> NOTE: When the policy that is governing the request has enabled **Allow simultaneous access** for multiple user access, the request may still be available even though **Show Account Request Availability** indicates it is in use.

The **My Request** page has additional settings that can be used to configure the displayed information. Clicking the button will open a panel with the following options:

- **My Request Favorites**: Select this option to display a widget showing configured favorite requests.
- **Show Account Request Availability (may impact performance)**: Select this option to show the account request availability. Depending on the number of requests this may impact performance.
- **Show Session Launch Button**: Select this option to add a **Launch Session** button the **My Request** page. This button allows you to open sessions via registered URL schemes in the browser.
- **Show Web Session Launch Button**: Select this option to add a **Launch Web Session** button the **My Request** page. This button allows you to open Safeguard Remote Access sessions via One Identity Starling.
- **Page Size**: Use the associated tiles (**25**, **50**, or **100**) to select the number of requests that will be displayed on the **My Request** page.

To make a request

You must be an authorized user of an entitlement to create a request for the assets and accounts you need.

1. Click **My Requests** to go to the **My Requests** page.
2. Follow the workflow steps. For more information, see Privileged access requests.

To create a favorite

You can create favorites for requests you make often. For more information, see Favorites (web client).

To view and manage requests

On the **My Requests** page, you can view the requests. Control the display using the following approaches:

- Click then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.
- Click **Sort By** then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.
- Click sort up or sort down to sort in ascending or descending order.
- Click **Filters** to filter by the status.
  - **Available**: Approved requests that are ready to view or copy.
  - **Pending Approval**: Requests that are waiting for approval.
  - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Sessions suspend feature.

    - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.
    - **Expired**: Requests for which the **Checkout Duration** has elapsed.
    - **Denied**: Requests denied by the approver.

- Click **Search** to see a list of searchable elements. Or enter search characters. For more information, see Search box.
- If a denied or revoked request has been commented on by an approver, you can click the button associated with the request to view the comment.

To launch web sessions

There are two options for launching browser-based sessions from the Safeguard for Privileged Sessions web client:

- **Launch Session**: This option allows you to open Windows desktop-based sessions via registered URL schemes.
- **Launch Web Session**: This button allows you to open Safeguard Remote Access sessions via One Identity Starling.

In order to use the **Launch Web Session** button to launch Safeguard Remote Access sessions, some additional requirements must be met:

- Safeguard for Privileged Sessions must be joined to Starling.
- Safeguard Remote Access and Safeguard for Privileged Sessions may have additional configuration requirements. For more information, see the Safeguard Remote Access and Safeguard for Privileged Sessions documentation.

Personal password vault

The personal password vault extends security and credential protection to business users to store and manage passwords. Users must have the **Personal Passwords** permission granted.

User benefits include:

- Users can store up to 100 personal passwords, set optional expiration dates, and share passwords.
- Users know at a glance the last time they changed their password.
- Users have a history of personal password changes. This is handy if the user changes the password in the vault but not on the target account or if the user needs to work from a backup.
- A password can be shared by the user with one other user. For example, when a user is not available they can give a coworker access to a password. Access can be revoked or the user that has the password shared can opt out of the share.

With the personal password vault, business user passwords are under the control of the IT and security teams, versus a variety of methods of storing passwords. Benefits of the personal password vault for Security Policy Administrators and User Administrators include:

- An organization sanctioned and controlled tool is used for users to store personal passwords.
- Personal passwords are secured and encrypted. They are stored separately from managed account passwords.
- The personal password vault audits the retrieval and change of passwords so administrators know when users pulled information from the vault.
- Administrators can recover passwords when someone leaves the company. The administrator must change the authentication provider to local, set the password of the user, and then log in and view the personal password vault.
- There is no way to recover the personal password vault of a deleted user.

System users (like the bootstrap admin) cannot create personal accounts.

> IMPORTANT: The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Directory Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Directory Groups from which they inherited it, the user will no longer be able to access **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission again, they regain access to all of their existing data.

For more information, see Permissions tab (add user) on page 545.

The **Personal Password Vault** page toolbar functions follow.

Table 13: Personal Password Vault: Toolbar

Option	Description
+ **New Entry**	Add an entry to the to the personal password vault.
- **Remove Entry**	Remove one or more selected entries from the personal password vault. Once an entry is removed, you will not have access to the credentials.
Edit Entry	Modify the selected entry.
Information	View information about the selected entry including: • **Name**: A meaningful name assigned to the application or account to access. **Account Name**: The user name for log on authentication. Click **Copy Account Name** to copy the name to your clipboard.

Option	Description
	Password: The secret which you can **Show** or **Hide** as well as copy by clicking **Copy Password**. **Expires**: The date the password is no longer valid. • **Notes**: Information for the user and anyone sharing the password, such as secondary secrets or other instructions. • **Sharing**: The user name of the person your password is **Shared With** and the date the **Sharing Expires**. To change the **Sharing Expires** date, click **Edit**, change the date and then click **Save**.
Share Credentials	Select one or more entries then select the user you want to share credentials with and the date to stop sharing. Users must have this feature enabled to be listed. For more information, see Permissions tab (add user) on page 545.
Stop Sharing	Select one or more entries then click **Stop Sharing**. If a password is shared by another owner with you, you cannot remove the share but you can opt yourself out of the share.
History	Thirty days of password history display as a default. You can set a date range for displaying password history by selecting **From** and **To** values using the calendar. Or, you can click **Date Range** to select set time periods for hours, days, months, or **All History**. In addition to viewing the Date Changed, you can can **Show** or **Hide** the password or **Copy Password**.
Copy Account Name	Copy the account name of the selected entry.
Copy Password	Copy the password of the selected entry.
Open URL	Click to open the URL web address entered when the password was added or edited.
Columns	Click to select the columns you want to display.

Option	Description
Search	Click to see a list of searchable elements. Or enter search characters. For more information, see Search box.

Entry details for various applications and systems display in the grid.

Table 14: Personal Password Vault: Passwords grid

Name	A meaningful name given to the application or account to access, for example Company Twitter.
Account Name	The user name used for log on authentication.
Expires	The date the password expires or blank (no value) if the password does not have an expiration date.
Shared	Display all the following values or click the filter to select a few values to display: • **Not Shared** if the password is not shared with another user. • **Shared** if you are sharing the password with another user. • **Shared with Me** if another user is sharing their password with you.
Shared With	The user name (and domain name, if applicable) with whom the password is shared; blank if the password is not shared. You can hover over the user name to see the email address for verification.
Owner	The owner of the password.
Sharing Expires	The date sharing expires and the password will no longer be available to the **Shared With** user.

To add a password

1. On the **Personal Password Vault** page, click **New Entry**.
2. Enter the following values.
   a. **Name**: Enter a meaningful name for the application or account to access, for example Company Twitter.
   b. **Account Name**: Enter the user name you use to log on for authentication.
   c. **Password**: You can type in a password or automatically generate a password. Adding a password is optional. For example, you may want to store information about an application or system in the **Notes** and not store the actual password. The **Notes** limit is 2000 characters.

- If you type in the password, you can click **Show** or **Hide** to view the entry or not. You can also click **Copy Password** to copy the password to your clipboard.
- To automatically generate a password, click **Generate a password**. The password is automatically generated. You can change password rules:
  i. **Length**: Use the slider or enter a value to reset the required length.
  ii. **Numbers**: Toggle the requirement to use numbers in the password on or off. The password is regenerated per the setting.
  iii. **Symbols**: Toggle the requirement to use symbols in the password on or off. The password is regenerated per the setting.
  iv. Click **Regenerate** to generate a new password.
  v. Click **OK** to save the generated password.
  vi. Back on the New Entry panel, you can click **Copy Password** to copy the password to your clipboard.

d. **Expires**: It is recommended that you set an expiration date to protect your access. You can enter the date or click the calendar to select a date.

e. **URL**: Enter the web address of the application or system, for example, Amazon.com. Click **Open URL** to test the link. You can also **Copy** the URL.

f. **Notes**: Enter any free form notes that are helpful for you or for the person with whom you may share the password. You can also use **Notes** for information about an application or system, such as certifications or keys. The limit is 2000 characters.

3. Click **Save**.

To share your password with another user

1. On the **Personal Password Vault** page in the grid, select one or more entries to share.
2. Click **Share Credentials**.
3. On the **Share Credentials** dialog, click **Browse**.
4. On the **Share With...** dialog, users with Personal Passwords permissions are available including their **Display Name**, **Domain**, and **Email Address**. Administrators can add permissions. For more information, see Permissions tab (add user) on page 545.

   Select one user. To search for a user, enter a value in the **Search** text box or click the icon then make a selection to search by **Domain**, **Display Name**, or **Email**

Address. Enter the first letters of the value to display the matches and select the user.
Click **OK**.

5. Set the sharing end date which must be between one day and one year. In **Stop Sharing**, enter the date, click the calendar and select the date, or click **Sharing Expires** to select a week or month interval. The password will not be available to the user on that date.
6. Click **Share**.

One easy way to change the **Sharing Expires** date later is to select the entry and click **Information**. Next to the **Sharing Expires** field, click **Edit**, change the **Sharing Expires** date, then click **Save**.

To stop sharing your password with another user

1. On the **Personal Password Vault** grid, the Shared column displays **Shared** if you are sharing the password.
2. Select one or more check boxes of entries to stop sharing.
3. Click **Stop Sharing**. The **Stop Sharing** dialog displays as a warning.
4. Click **Stop Sharing**.

Approvals

Click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see. You can select columns including:
  - **Action**: Displays **Approve only this request** and **Deny only this request**.

- **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).
- **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, **API Key**, or **Telnet**).
- **Account**: Displays the managed account name.
- **Ticket Number**: Displays the ticket number, if required.
- **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).

- **Search**: For more information, see Search box on page 78.

Reviews

Select **Reviews** on the left of the page to manage reviews. On the **Reviews** page, you can:

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click **Mark all the selected requests as reviewed**.
  - If a comment is needed, this icon will display as **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
  - **Action**: Displays **This request requires review comments** or **Mark only this request as reviewed**.
  - **Requester**: Displays the user name of the requester.
  - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, **API Key**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.
  - **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 78.

Favorites

Favorites are located on your **Home** or **My Requests** page. For systems and accounts that are used often, you can save the access request as a favorite. Favorites are similar to bookmarks in a web browser, allowing you to save any access request, consisting of one or more assets and accounts, as well as the access type, for example, password or RDP, so the next time you can open it with a single click.

To create favorites, on the **My Requests** page, you can:

- Create a favorite by using the tree view control on the page (without having to submit an access request).
- Save the request as a favorite during the process of creating and submitting a new access request.

On your **Home** page, 5 of your most recently used favorites are listed. This list is automatically maintained based on your usage.

To create and manage favorites using the tree view control

1. Next to a folder, click the **context menu** and select one of the following:
   - To create a new folder for organization purposes, click **New Folder**.
   - To create a new favorite in the selected folder, click **New Favorite**.

   NOTE: By default, the new favorite will be created in the selected folder. However, you can move it to a different folder. For more information, see To add a favorite.
2. To display the tree view either in a single pane, or split pane view, click .
3. To find any favorite or folder based on the name, asset name, or account name, use **Search**.
4. To edit a favorite, click the favorite. A dialog will be displayed. Click **Edit Favorite**.
5. Each folder has a **context menu** next to it. Clicking the **context menu** allows you to do the following:
   a. To create a new favorite, click **New Favorite**. By default, the new favorite will be created in the selected folder.
   b. To create a new folder, click **New Folder**. You can nest multiple folders within a folder.
   c. To rename the folder, click **Rename**.
   d. To delete the entire folder and all of its contents, including nested folders and favorites, click **Delete**.
   e. To collapse the folder and all of its nested folders, click **Collapse**.
   f. To expand the folder and all of its nested folders, click **Expand**.
6. To reorder favorites or folders, or to move them into other folders, drag and drop them.

To add a favorite

1. To add a new favorite in the selected folder, click the ⋮ **context menu** next to a folder.
2. On the **New Favorite** page, select one or more assets and accounts. To quickly find an asset or account, use one of the following approaches:
   - Click **Search** to search the **Asset**, **Network Address**, or **Platform**. You an also enter a search word or phrase. For more information, see Search box.
   - The number of **Items Selected** will be displayed in the lower left corner.
   - In the lower right corner, select the number of **Items per page** to display. Click the arrows to move through the pages.
3. Click **Next**.
4. On **Favorite Details**, enter a name for the favorite.
5. Select the color that will be used when displaying the favorite on the **Home** and **My Requests** pages.
6. Click **Save Favorite**.

   The access request is then added to your **Favorites**. After a favorite is created, you can use and make changes to your favorites by selecting it from **Favorites** on the **Home** page or the **My Requests** page.

NOTE: Favorites have unique links, so you can bookmark or copy the link and later access it via that link rather than navigating through the web client.

NOTE: You must be authorized to create requests for the assets and accounts you choose to include in a favorite. To change the look of the favorite tiles, click for grid view or for list view.

If **Show Account Availability** is enabled, you can identify if a privileged account is available or not. Accounts display a warning badge if in use by a request. An account's status is updated immediately after being changed in order to avoid overlapping account requests from multiple users. Hover over the badge to display `<X> of <X> accounts in use`. Showing account availability requires additional API queries that may impact performance. This toggle is set by the user, not an administrator. There is no global toggle.

NOTE: When the policy that is governing the request has enabled **Allow simultaneous access** for multiple user access, the request may still be available even though **Show Account Request Availability** indicates it is in use.

Privileged access requests

One Identity Safeguard for Privileged Passwords provides a workflow engine that supports time restrictions, multiple approvers, reviewers, emergency access, and expiration of policy. It also includes the ability to input reason codes and integrate directly with ticketing systems.

In order for a request to progress through the workflow process, authorized users perform assigned tasks. These tasks are performed from the user's **Home** page.

As a SPP user, your **Home** page provides a quick view to the access request tasks that need your immediate attention. In addition, an Administrator can set up alerts to be sent to users when there are pending tasks needing attention. For more information, see Configuring alerts on page 95.

The access request tasks you see on your **Home** page depend on the rights and permissions you have been assigned by an entitlement's access request policies. For example:

- Requesters see tasks related to submitting new access requests, as well as actions to be taken once a request has been approved (for example, viewing passwords, copying passwords, launching sessions, and checking in completed requests).

  Requesters can also define favorite requests, which may appear on their **Home** page and **My Requests** page for subsequent use.
- Approvers see tasks related to approving (or denying) and revoking access requests.
- Reviewers see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

The following three workflows are available:

- Password release request workflow
- SSH key release request workflow
- API key release request workflow
- Session request workflow

Configuring alerts

All users are subscribed to the following email notifications; however, users will not receive email notifications unless they have been included in a policy as a requester (user), approver, or reviewer.

Email notifications

You must configure One Identity Safeguard for Privileged Passwords properly for users to receive email notifications:

- For Local users, you must set your email address correctly in **My Settings**. For more information, see My Settings.
- For Directory users, set your email correctly in the directory where your user resides.
- The Security Policy Administrator must configure the access request policies to notify people of pending access workflow events (that is, pending approvals and pending reviews). For more information, see Creating an access request policy.
- Contact your Security Policy Administrator to ensure the access request policies are configured to notify people of pending access workflow events.
- The Appliance Administrator must configure the SMTP server. For more information, see Enabling email notifications.
- Contact your Appliance Administrator to ensure the SMTP server is configured for email notifications.

Role-based email notifications generated by default

One Identity Safeguard for Privileged Passwords can be configured to send email notifications warning you of operations that may require investigation or action. Your administrative permissions determine which email notifications you will receive by default.

> NOTE: SPP administrators can use the following API to turn off these built-in email notifications:
>
> `POST /service/core/v3/Me/Subscribers/{id}/Disable`
>
> In addition, SPP administrators can subscribe to additional events based on their administrative permissions using the following API:
>
> `POST /service/core/v3/EventSubscribers`

Password release request workflow

One Identity Safeguard for Privileged Passwords provides secure control of managed accounts by storing account passwords until they are needed, and releases them only to

authorized persons. Then, SPP automatically updates the account passwords based on configurable parameters.

Typically, a password release request follows this workflow.

1. **Request**: Users that are designated as an authorized user of an entitlement can request passwords for any account in the scope of that entitlement's policies.
2. **Approve**: Depending on how the Security Policy Administrator configured the policy, a password release request will either require approval by one or more SPP users, or be auto-approved. This process ensures the security of account passwords, provides accountability, and provides dual control over the system accounts.
3. **Review**: The Security Policy Administrator can optionally configure an access request policy to require a review of completed password release requests for accounts in the scope of the policy.

Requesting a password release

If you are designated as an authorized user of an entitlement, you can request passwords for any account in the scope of the entitlement's policies.

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending password release workflow events, such as when a password release request is pending, denied, or revoked, and so forth. For more information, see Configuring alerts.

To request a password release

1. Click **Home** then **New Request** or open the **My Requests** page then click **New Request**.

   NOTE: You can also submit an access request from your **Favorites** pane, if you previously saved it as a favorite.

2. On the **New Access Request** page, select the accounts to be included in the access request and the type of access being requested for each selected account. You can search for accounts based on asset information. The assets available for selection are based on the scope defined in the entitlement's access request policies.

   NOTE: Use the button to select the columns to display.

   - **Asset**: The display name of the managed system.
   - **Account**: All available accounts will be listed in the **Account** column.

     If **Show Account Availability** is enabled, you can identify if a privileged account is available or not. Accounts display a warning badge if in use by a request. An account's status is updated immediately after being changed in order to avoid overlapping account requests from multiple users. Hover over the badge to display `<X> of <X> accounts in use`. Showing account availability

requires additional API queries that may impact performance. This toggle is set by the user, not an administrator. There is no global toggle.

> NOTE: When the policy that is governing the request has enabled **Allow simultaneous access** for multiple user access, the request may still be available even though **Show Account Request Availability** indicates it is in use.

- **Access Type**: The type of access request appears in the **Access Type** column. If the type is a drop-down, multiple access request types are available. Open the drop-down and select the access type, for example, **Password**, **RDP**, **SSH**, **SSH Key**, or **Telnet**.
- **Account Description**: (When applicable) The description of the account.
- **Asset Description**: (When applicable) The description of the asset.

You can remove an account from the list by clearing the check box associated with an entry in the grid.

3. Click **Next**.
4. On **Request Details**, configure the following settings, which will apply to all of the selected assets and accounts:
   a. **Emergency Access**: If the policy has emergency access enabled, select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval. For more information, see Creating an access request policy.
   b. **When**: Select one of the following options:
      i. **Now**: If selected, the request is immediately created.
      ii. **Later**: If selected, fields will appear allowing you to enter a specific date and time for the request in the user's local time.
   c. **How Long**: Based on the policy, do one of the following:
      - View the **Checkout Duration**.
      - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy. For more information, see Creating an access request policy.
   d. **Ticket Number**: If the policy requires a ticket number, enter a ticket number. If multiple accounts are in the request and one or more require a ticket number, the ticket number is applied to all of the requests associated with this access request. For more information, see Ticket systems.
   e. **Reason**: If the policy requires a reason, enter a reason. If multiple accounts are in the request and one or more require a reason. The reason is applied to all of the requests associated with this access request. For more information, see Reasons.

      Select the **Description** down arrow to view the description defined for the selected reason.

f. **Comment**: If required, enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 1000 characters.

5. To save the access request as a favorite, select the **Save this request as a favorite** check box and enter a name for the request.

   This access request is then added to your **Favorites**. In the web client, favorites are displayed on the **Home** page and the **My Requests** page.

6. After entering the required information, click **Submit Request**.

   Additional information displays if the access requests submitted were unsuccessful with information on how to address the issues. Once they have been addressed, you can resubmit the request.

When the request has been approved, you can use the password. For more information, see Taking action on a password release request.

Taking action on a password release request

The actions that can be taken on a password release request depends on the state of the request.

To take action on a password release request

1. From the web client, click **My Requests**. Use any of the following methods to control the request displayed:

   - Click then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.
   - Click **Sort By** then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.
   - Click sort up or sort down to sort in ascending or descending order.
   - Click **Filters** to filter by the status.
     - **Available**: Approved requests that are ready to view or copy.
     - **Pending Approval**: Requests that are waiting for approval.
     - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Sessions suspend feature.
     - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.

    - **Expired**: Requests for which the **Checkout Duration** has elapsed.
    - **Denied**: Requests denied by the approver.
  - Click **Search** to see a list of searchable elements. Or enter search characters. For more information, see Search box.
  - If a denied or revoked request has been commented on by an approver, you can click the button associated with the request to view the comment.
2. You can take any of the following actions on the password release request:
  - Available Password request:
    - The name, account, and remaining time is displayed.
    - If your browser allows, click **Copy** to check out the password. This puts the password onto your clipboard, ready for you to use. Or, click **Show** to check out the password and view the password. A password displays on your screen for 20 seconds. The web client displays up to 10,000 characters before truncating the password, however the API allows any set password payload below 1MB. If the password changes while you have it checked out, and your current request is still valid, select either **Copy** or **Show** again to obtain the new password.
    - Select **Hide** to conceal the information from view.
    - Once you are done working, click **Check-In Request** to complete the password check out process.
  - Available Password Request with time-based one-time password (TOTP) configured (for more information, see Setting a TOTP authenticator):
    - Click **Copy MFA Code (OTP)** to put the TOTP onto your clipboard, or **View MFA Code (OTP)** if you want to manually enter the TOTP. Clicking either button will check out the active TOTP and initiate a countdown during which the TOTP must be used.
    - Depending on the platform, you may need to enter multiple TOTP. Each successive TOTP will be made available once the previous TOTP has expired. If the TOTP changes while you have it checked out, and your current request is still valid, select either **Copy MFA Code (OTP)** or **View MFA Code (OTP)** again to obtain the TOTP, if enabled by your Administrator.
    - Once you are done working, click **Check-In Request** to complete the password check out process.
  - **Approved** request: Select **Cancel Request** to remove the request.

    A password release request changes from **Approved** to **Available** when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.

- **Pending** request: Select **Cancel Request** to remove the request.
- **Revoked** request: Select **Resubmit** to request the password again.
- **Expired** request: Select **Remove Request** to delete the request from the list.
- **Denied** request: Select **Resubmit** to request the password again.

  Select **Remove Request** to delete the request from the list.

Approving a password release request

Depending on how the Security Policy Administrator configured the policy, a password release request will either require approval by one or more SPP users, or be auto-approved. This process ensures the security of account passwords, provides accountability, and provides dual control over the system accounts.

You can revoke a request between the time the requester views it and checks it in.

Any eligible approver can deny a password release request after it has already been approved or auto-approved. Once disallowed, the requester will no longer have access to the password, but they are given another opportunity to request that password again. The requester receives an email notifying them that the request was denied.

SPP can be configured to notify you of a password release request that requires your approval. For more information, see Configuring alerts on page 95.

To approve or deny a password release request

Click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see. You can select columns including:
  - **Action**: Displays **Approve only this request** and **Deny only this request**.
  - **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).

- **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, **API Key**, or **Telnet**).
- **Account**: Displays the managed account name.
- **Ticket Number**: Displays the ticket number, if required.
- **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).

- **Search**: For more information, see Search box on page 78.

Reviewing a completed password release request

The Security Policy Administrator can configure an access request policy to require a review of completed password release requests for accounts in the scope of the policy.

You can configure SPP to notify you of a password release request that requires your review. For more information, see Configuring alerts on page 95.

To review a completed password release request

Select **Reviews** on the left of the page to manage reviews. On the **Reviews** page, you can:

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click **Mark all the selected requests as reviewed**.
  - If a comment is needed, this icon will display as **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
  - **Action**: Displays **This request requires review comments** or **Mark only this request as reviewed**.
  - **Requester**: Displays the user name of the requester.
  - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, **API Key**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.

- **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 78.

SSH key release request workflow

One Identity Safeguard for Privileged Passwords provides secure control of managed accounts by storing SSH keys until they are needed, and releases them only to authorized persons. Then, SPP automatically updates the account SSH keys based on configurable parameters.

Typically, an SSH key release request follows this workflow.

1. **Request**: Users that are designated as an authorized user of an entitlement can request SSH keys for any account in the scope of that entitlement's policies.
2. **Approve**: Depending on policy configuration, approval can be automatic or require the consent of one or more users which provides closer control over system accounts.
3. **Review**: The Security Policy Administrator can optionally configure an access request policy to require a review of completed SSH key release requests for accounts in the scope of the policy.

Requesting an SSH key release

If you are designated as an authorized user of an entitlement, you can request SSH keys for any account in the scope of the entitlement's policies.

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending SSH key release workflow events, such as when an SSH key release request is pending, denied, or revoked, and so forth. For more information, see Configuring alerts on page 95.

To request an SSH key release

1. Click **Home** then **New Request** or open **My Requests** then click **+ New Request**.

   NOTE: You can also submit an access request from your **Favorites** pane, if you previously saved it as a favorite.

2. On the **New Access Request** page, select the accounts to be included in the access request and the type of access being requested for each selected account. You can search for accounts based on asset information. The assets available for selection are based on the scope defined in the entitlement's access request policies.
3. NOTE: Use the button to select the columns to display.

- **Asset**: The display name of the managed system.
- **Account**: The available account appears in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.
- **Access Type**: The type of access request appears in the **Access Type** column. If the type is a drop-down, you can click the drop-down then multiple access request types are available. Click the drop-down and select the access type, in this case, **SSH Key**.
- **Account Description**: (When applicable) The description of the account.
- **Asset Description**: (When applicable) The description of the asset.

You can remove an asset or account from the list by clearing the check box associated with an entry in the grid.

4. Click **Next**.
5. On **Request Details**, configure the following settings, which will apply to all of the selected assets and accounts:
   a. **Emergency Access**: If the policy has emergency access enabled, select this option to gain immediate emergency access to this SSH key. When you use **Emergency Access**, the request requires no approval. For more information, see Creating an access request policy.
   b. **When**: Select one of the following options:
      i. **Now**: If selected, the request is immediately created.
      ii. **Later**: If selected, fields will appear allowing you to enter a specific date and time for the request in the user's local time.
   c. **How Long**: Based on the policy, do one of the following:
      - View the **Checkout Duration**.
      - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy. For more information, see Creating an access request policy.
   d. **Ticket Number**: If the policy requires a ticket number, enter a ticket number. If multiple accounts are in the request and one or more require a ticket number, the ticket number is applied to all of the requests associated with this access request. For more information, see Ticket systems on page 238.
   e. **Reason**: If the policy requires a reason, enter a reason. If multiple accounts are in the request and one or more require a reason. The reason is applied to all of the requests associated with this access request. For more information, see Reasons on page 534.

      Select the **Description** down arrow to view the description defined for the selected reason.

f. **Comment**: If required, enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 1000 characters.

6. To save the access request as a favorite, select the **Save this request as a favorite** check box and enter a name for the request.

   This access request is then added to your **Favorites**. In the web client, favorites are displayed on the **Home** page and the **My Requests** page.

7. After entering the required information, click **Submit Request**.

   Additional information displays if the access requests submitted were unsuccessful with information on how to address the issues. Once they have been addressed, you can resubmit the request.

When the request has been approved, you can use the SSH key. For more information, see Taking action on an SSH key release request on page 104.

Taking action on an SSH key release request

The actions that can be taken on an SSH key release request depends on the state of the request.

To take action on an SSH key release request

1. From the web client, click **My Requests**. Use any of the following methods to control the request displayed:

   - Click then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.
   - Click **Sort By** then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.
   - Click sort up or sort down to sort in ascending or descending order.
   - Click **Filters** to filter by the status.
     - **Available**: Approved requests that are ready to view or copy.
     - **Pending Approval**: Requests that are waiting for approval.
     - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Sessions suspend feature.
     - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.

    - **Expired**: Requests for which the **Checkout Duration** has elapsed.
    - **Denied**: Requests denied by the approver.
  - Click **Search** to see a list of searchable elements. Or enter search characters. For more information, see Search box.
  - If a denied or revoked request has been commented on by an approver, you can click the button associated with the request to view the comment.
2. You can take any of the following actions on the SSH key release request:
  - Available request:
    a. The name, account, and remaining time is displayed. Click on the tile to see additional information or use the **Fetch SSH Details** button.
    b. The **Format** displays and can be selected, if necessary. Formats include **OpenSSH**, **SSH2**, and **PuTTY**. The **Format** chosen is preselected as the default for the next access request.
    c. Click **Checkout SSH Key** to check out the SSH key. This puts the SSH key onto your clipboard, ready for you to use.
    d. Click **Start SSH Session** to launch the session.
    e. **Private Key**: You can click **Save** or **Copy**.
    f. **Passphrase**: You can click **Show** or **Copy** if **Passphrase Protect SSH Key** was selected on when creating an access request policy.
    g. The following types of information may display based on the format you select.
      - **SHA-1 Fingerprint**
      - **MD5 Fingerprint**
      - **Public Key**: You can click **Save** or **Copy**.

      If the SSH key changes while you have it checked out, and your current request is still valid, you can select the following to obtain an new SSH key, as available: **Save**, **Copy**, or **Show**.
    h. Once you are done working, click **Check-In Request** to complete the SSH key check out process.
  - **Approved** request: Select **Cancel Request** to remove the request.

    An SSH key release request changes from **Approved** to **Available** when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
  - **Pending** request: Select **Cancel Request** to remove the request.

- **Revoked** request: Select **Resubmit** to request the SSH key again.

  Select **Remove** to delete the request from the list.

- **Expired** request: Select **Remove Request** to delete the request from the list.
- **Denied** request: Select **Resubmit** to request the SSH key again.

  Select **Remove Request** to delete the request from the list.

Approving an SSH key release request

Depending on how the Security Policy Administrator configured the policy, an SSH key release request will either require approval by one or more SPP users, or be auto-approved. Depending on policy configuration, approval can be automatic or require the consent of one or more users which provides closer control over system accounts.

You can revoke a request between the time the requester views it and checks it in.

Any eligible approver can deny an SSH key release request after it has already been approved or auto-approved. Once disallowed, the requester will no longer have access to the SSH key, but they are given another opportunity to request that SSH key again. The requester receives an email notifying them that the request was denied.

SPP can be configured to notify you of an SSH key release request that requires your approval. For more information, see Configuring alerts on page 95.

To approve or deny an SSH key release request

Click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see. You can select columns including:
  - **Action**: Displays **Approve only this request** and **Deny only this request**.
  - **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).

- **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, **API Key**, or **Telnet**).
- **Account**: Displays the managed account name.
- **Ticket Number**: Displays the ticket number, if required.
- **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).

- **Search**: For more information, see Search box on page 78.

Reviewing a completed SSH key release request

The Security Policy Administrator can configure an access request policy to require a review of completed SSH key release requests for accounts in the scope of the policy.

You can configure SPP to notify you of an SSH key release request that requires your review. For more information, see Configuring alerts on page 95.

To review a completed SSH key release request

Select **Reviews** on the left of the page to manage reviews. On the **Reviews** page, you can:

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click **Mark all the selected requests as reviewed**.
  - If a comment is needed, this icon will display as **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
  - **Action**: Displays **This request requires review comments** or **Mark only this request as reviewed**.
  - **Requester**: Displays the user name of the requester.
  - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, **API Key**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.

- **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 78.

API key release request workflow

One Identity Safeguard for Privileged Passwords provides secure control of managed accounts by storing API keys associated with Azure AD and AWS connectors until they are needed, and releases them only to authorized persons. Then, SPP automatically updates the account API keys based on configurable parameters.

Typically, an API key release request follows this workflow.

1. **Request**: Users that are designated as an authorized user of an entitlement can request API keys for any account in the scope of that entitlement's policies.
2. **Approve**: Depending on policy configuration, approval can be automatic or require the consent of one or more users which provides closer control over system accounts.
3. **Review**: The Security Policy Administrator can optionally configure an access request policy to require a review of completed API key release requests for accounts in the scope of the policy.

Requesting an API key release

If you are designated as an authorized user of an entitlement, you can request API keys for any account in the scope of the entitlement's policies.

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending API key release workflow events, such as when an API key release request is pending, denied, or revoked, and so forth. For more information, see Configuring alerts on page 95.

To request an API key release

1. Click **Home** then **New Request** or open **My Requests** then click **+ New Request**.

   NOTE: You can also submit an access request from your **Favorites** pane, if you previously saved it as a favorite.

2. On the **New Access Request** page, select the accounts to be included in the access request and the type of access being requested for each selected account. You can search for accounts based on asset information. The assets available for selection are based on the scope defined in the entitlement's access request policies.
3. NOTE: Use the button to select the columns to display.

- **Asset**: The display name of the managed system.
- **Account**: The available account appears in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.
- **Access Type**: The type of access request appears in the **Access Type** column. If the type is a drop-down, you can click the drop-down then multiple access request types are available. Click the drop-down and select the access type, in this case, **API Key**.
- **Account Description**: (When applicable) The description of the account.
- **Asset Description**: (When applicable) The description of the asset.

You can remove an asset or account from the list by clearing the check box associated with an entry in the grid.

4. Click **Next**.
5. On **Request Details**, configure the following settings, which will apply to all of the selected assets and accounts:
   a. **Emergency Access**: If the policy has emergency access enabled, select this option to gain immediate emergency access to this API key. When you use **Emergency Access**, the request requires no approval. For more information, see Creating an access request policy.
   b. **When**: Select one of the following options:
      i. **Now**: If selected, the request is immediately created.
      ii. **Later**: If selected, fields will appear allowing you to enter a specific date and time for the request in the user's local time.
   c. **How Long**: Based on the policy, do one of the following:
      - View the **Checkout Duration**.
      - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy. For more information, see Creating an access request policy.
   d. **Ticket Number**: If the policy requires a ticket number, enter a ticket number. If multiple accounts are in the request and one or more require a ticket number, the ticket number is applied to all of the requests associated with this access request. For more information, see Ticket systems on page 238.
   e. **Reason**: If the policy requires a reason, enter a reason. If multiple accounts are in the request and one or more require a reason. The reason is applied to all of the requests associated with this access request. For more information, see Reasons on page 534.

      Select the **Description** down arrow to view the description defined for the selected reason.

f. **Comment**: If required, enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 1000 characters.

6. To save the access request as a favorite, select the **Save this request as a favorite** check box and enter a name for the request.

   This access request is then added to your **Favorites**. In the web client, favorites are displayed on the **Home** page and the **My Requests** page.

7. After entering the required information, click **Submit Request**.

   Additional information displays if the access requests submitted were unsuccessful with information on how to address the issues. Once they have been addressed, you can resubmit the request.

When the request has been approved, you can use the API key. For more information, see Taking action on an API key release request.

Taking action on an API key release request

The actions that can be taken on an API key release request depends on the state of the request.

To take action on an API key release request

1. From the web client, click **My Requests**. Use any of the following methods to control the request displayed:

   - Click then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.
   - Click **Sort By** then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.
   - Click sort up or sort down to sort in ascending or descending order.
   - Click **Filters** to filter by the status.
     - **Available**: Approved requests that are ready to view or copy.
     - **Pending Approval**: Requests that are waiting for approval.
     - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Sessions suspend feature.
     - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.

    - **Expired**: Requests for which the **Checkout Duration** has elapsed.
    - **Denied**: Requests denied by the approver.
  - Click **Search** to see a list of searchable elements. Or enter search characters. For more information, see Search box.
  - If a denied or revoked request has been commented on by an approver, you can click the button associated with the request to view the comment.
2. You can take any of the following actions on the API key release request:
  - Available request: If the API key changes while you have it checked out, and your current request is still valid, select **Copy** or **Show** again to obtain the new API key, if enabled by your Administrator.
    - The name, account, and remaining time is displayed.
    - Click **Copy** to check out the **API Key**. This puts the value onto your clipboard, ready for you to use. Since you are not limited to a single API key per account, you may see additional keys listed.
    - In addition, depending on the platform, you can copy the **Client Identifier**, **Client Secret**, or **Client Secret Identifier** by clicking the **Copy** button associated with each field. Click **Show** to view the information without copying, and **Hide** to conceal the information from view.
    - Once you are done working, click **Check-In Request** to complete the password check out process.
  - **Approved** request: Select **Cancel Request** to remove the request.

    An API key release request changes from **Approved** to **Available** when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
  - **Pending** request: Select **Cancel Request** to remove the request.
  - **Revoked** request: Select **Resubmit** to request the API key again.

    Select **Remove** to delete the request from the list.
  - **Expired** request: Select **Remove Request** to delete the request from the list.
  - **Denied** request: Select **Resubmit** to request the API key again.

    Select **Remove Request** to delete the request from the list.

Approving an API key release request

Depending on how the Security Policy Administrator configured the policy, an API key release request will either require approval by one or more SPP users, or be auto-approved. Depending on policy configuration, approval can be automatic or require the consent of one or more users which provides closer control over system accounts.

You can revoke a request between the time the requester views it and checks it in.

Any eligible approver can deny an API key release request after it has already been approved or auto-approved. Once disallowed, the requester will no longer have access to the API key, but they are given another opportunity to request that API key again. The requester receives an email notifying them that the request was denied.

SPP can be configured to notify you of an API key release request that requires your approval. For more information, see Configuring alerts on page 95.

To approve or deny an API key release request

Click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see. You can select columns including:
  - **Action**: Displays **Approve only this request** and **Deny only this request**.
  - **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).
  - **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, **API Key**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.
  - **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 78.

Reviewing a completed API key release request

The Security Policy Administrator can configure an access request policy to require a review of completed API key release requests for accounts in the scope of the policy.

You can configure SPP to notify you of an API key release request that requires your review.

To review a completed API key release request

Select **Reviews** on the left of the page to manage reviews. On the **Reviews** page, you can:

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click **Mark all the selected requests as reviewed**.
  - If a comment is needed, this icon will display as **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
  - **Action**: Displays **This request requires review comments** or **Mark only this request as reviewed**.
  - **Requester**: Displays the user name of the requester.
  - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, **API Key**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.
  - **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 78.

Session request workflow

Authorized users can authorize connections, view active connections, limit access to specific resources, be alerted if connections exceed pre-set time limits, and even close connections.

Typically a session request follows the workflow below:

1. **Request**: Users that are designated as an authorized user of an entitlement can request a session for any asset in the scope of that entitlement's policies.
2. **Approve**: Depending on how the Security Policy Administrator configured the policy, a session request will either require approval by one or more SPP users, or be auto-approved.
3. **Review**: The Security Policy Administrator can optionally configure an access request policy to require a review of completed requests for assets in the scope of the policy. In addition, if session recording is enabled in the policy, reviewers can audit the workflow transactions and launch the Desktop Player to replay the session as part of the review process.

About sessions and recordings

One Identity Safeguard for Privileged Passwords proxies all sessions to target resources. Users do not have direct access to resources, therefore, the enterprise is protected against viruses, malware or other dangerous items on the user's system. Safeguard can proxy and record Unix/Linux, Windows, network devices, firewalls, routers and more.

> NOTE: PuTTY is used to launch the SSH client for SSH session requests and MSTSC is used for RDP session requests. For information on how to setup using PuTTY or MSTSC, see SCALUS.

Important notes

- Sessions requests are enabled by default. However, if authorized users cannot request sessions, check the **Session Requests** setting in the web client.

  > NOTE: You must have Appliance Administrator permissions to manage the service settings.

- All session activity (every packet sent and action that takes place on the screen, including mouse movements, clicks, and keystrokes) is recorded and available for play back.
- If SPP detects no activity for 10 minutes during a privileged session, the session is closed.

Requesting session access

If you are designated as an authorized user of an entitlement, you can request access for a specific period (or session) to any account or asset in the scope of the entitlement's policies.

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending access request workflow events, such as when a session request is pending, denied, or revoked, and so on. For more information, see Configuring alerts on page 95.

To request session access

1. Click **Home** then **New Request** or open **My Requests** then click **+ New Request**.

   NOTE: You can also submit an access request from your **Favorites** pane, if you previously saved it as a favorite.

2. On the **New Access Request** page, select the accounts to be included in the access request and the type of access being requested for each selected account. You can search for accounts based on asset information. The assets available for selection are based on the scope defined in the entitlement's access request policies.

   If an `SPS_Initiated` connection policy is selected when creating an access request, the assets associated by that request will not display. The session-related access policy assigned to `SPS_Initiated` is filtered out. A connection policy other that `SPS_Initiated` must be selected to create an Access Request for the asset.

   NOTE: Use the button to select the columns to display.

   - **Asset**: The display name of the managed system.
   - **Account**: The available account appears in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.

     If **Show Account Availability** is enabled, you can identify if a privileged account is available or not. Accounts display a warning badge if in use by a request. An account's status is updated immediately after being changed in order to avoid overlapping account requests from multiple users. Hover over the badge to display `<X> of <X> accounts in use`. Showing account availability requires additional API queries that may impact performance. This toggle is set by the user, not an administrator. There is no global toggle.

     NOTE: When the policy that is governing the request has enabled **Allow simultaneous access** for multiple user access, the request may still be available even though **Show Account Request Availability** indicates it is in use.

   - **Access Type**: The type of access request appears in the **Access Type** column. If the type is a drop-down, multiple access request types are available. Select the hyperlink and select the access type.
   - **Account Description**: (When applicable) The description of the account.
   - **Asset Description**: (When applicable) The description of the asset.

   You can remove an asset or account from the list by clearing the check box associated with an entry in the grid.

3. Click **Next**.

4. On **Request Details**, configure the following settings, which will apply to all of the selected assets and accounts:

a. **Emergency Access**: If the policy has emergency access enabled, select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval. For more information, see Creating an access request policy.

b. **When**: Select one of the following options:

   i. **Now**: If selected, the request is immediately created.

   ii. **Later**: If selected, fields will appear allowing you to enter a specific date and time for the request in the user's local time.

c. **How Long**: Based on the policy, do one of the following:

   - View the **Checkout Duration**.
   - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy. For more information, see Creating an access request policy.

d. **Ticket Number**: If the policy requires a ticket number, enter a ticket number. If multiple accounts are in the request and one or more require a ticket number, the ticket number is applied to all of the requests associated with this access request. For more information, see Ticket systems on page 238.

e. **Reason**: If the policy requires a reason, enter a reason. If multiple accounts are in the request and one or more require a reason. The reason is applied to all of the requests associated with this access request. For more information, see Reasons on page 534.

   Select the **Description** down arrow to view the description defined for the selected reason.

f. **Comment**: If required, enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 255 characters.

5. To save the access request as a favorite, select the **Save this request as a favorite** check box and enter a name for the request.

   This access request is then added to your **Favorites**. In the web client, favorites are displayed on the **Home** page and the **My Requests** page.

6. After entering the required information, click **Submit Request**.

   Additional information displays if the access requests submitted were unsuccessful with information on how to address the issues. Once they have been addressed, you can resubmit the request.

When the request has been approved, you can use the password. For more information, see Taking action on a password release request on page 98.

If the session does not launch

In a rare event that the access request does not result in a launchable session request, the following notifications display:

- `Please try again. The linked sessions module state is currently down or may be in a locked state.` This message may mean one of the following:
  - SPP could not contact Safeguard for Privileged Sessions. Try again so the request can be redirected to another managed host in the Safeguard for Privileged Sessions cluster.
  - The Safeguard for Privileged Sessions configuration is locked. Try again because this condition is typically because the Safeguard for Privileged Sessions administrator is making configuration changes to the Safeguard for Privileged Sessions appliance at the same time that a new access request is being created or a session is being launched.
- `Missing the session connection policy.` or
  `The selected Access Request Policy cannot be used to initiate a session from SPP. The highest priority policy must be associated with a valid SPS connection policy.`
  Check the connection policy configuration. In the web client, go to **Security Policy Management** > **Entitlements** > (edit) > **Access Request Policies** to add a valid connection policy. Save the policy and recreate the access request.

Taking action on a session request

The actions a user authorized to request access to a privileged session can take depends on the state of the request.

To take action on a session request

1. From the web client, click **My Requests**.
2. Search to find what you need. For more information, see Search box on page 78.
3. Click **Filters** to filter by the status.
   - **All**: Requests in all states.
   - **Available**: Approved requests that are ready (that is, a session that can be launched).
   - **Pending Approval**: Requests that are waiting for approval.
   - **Approved**: Requests that have been approved, but the check out time has not arrived.
   - **Revoked**: Approved requests retracted by the approver.
     - The approver can revoke a request after it is available.
     - When a user with Security Policy Administrator permissions revokes a live session, the active session is closed.

- **Expired**: Requests for which the **Checkout Duration** has elapsed.
- **Denied**: Requests denied by the approver.

4. Depending on the type of request, additional information may be available by clicking the tile.
5. You can take the following actions on session requests, depending on the state.
    - Available request: If the password or SSH key changes while you have it checked out, and your current request is still valid, select either **Copy** or **Show** again to obtain the new password or SSH key, if enabled by your Administrator.
        - For SSH and RDP accounts:
            - The **Start RDP Session**/**Start SSH Session** options are available only if enabled by user preferences. Click to launch the SSH client or RDP connection. For more information, see Launching the SSH client or Launching an RDP session.
            - Click **Check-In** to complete the check out process once you have ended your session.
            - In addition, you can use the following buttons to view or copy information into the dialog that contains the credentials needed to launch the session.
                - Click **Copy** to check out and copy the credential.
                - Click **Show** to check out the credential and view the credential.
        - For telnet or TN3270/TN5250 over telnet accounts, the fields needed are based on the terminal service application in use:
        -
            - For a terminal service application that uses an inband connection string (like telnet), click **Copy** to copy the **Hostname Connection String** and check out the password or SSH key. Then, paste the information in the log in screen.
            - If the terminal service application requires more information for log in (for example, TN3270/TN5250 over telnet):
                - Click **Show** to display values that may include **Vault Address** (the SPP address), a one-time **Token**, **Username**, **Asset**, and **Sessions Module** (the Safeguard for Privileged Sessions address).
                - Click **Copy** by any of the values to copy a single value. Or, you can click **Copy** at the right of all values to copy the entire the connection string, if that is required by your terminal service application.
                - Paste the necessary information into your terminal service application.

- Click **Check-In Request** to complete the password or SSH key check out process. This makes the session request available to reviewers.
- Click **Hide** to conceal the information from view.

- **Approved**: Select **Cancel Request** to remove the request. A session request changes from Approved to Available when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
- **Pending**: Click **Cancel Request** to remove the request.
- **Revoked**:
  - Click **Resubmit** to request the password or SSH key again.
  - Click **Remove Request** to delete the request from the list.
- **Expired**: Click **Remove Request** to delete the request from the list.
- **Denied**:
  - Click **Resubmit** to request the password or SSH key again.
  - Click **Remove Request** to delete the request from the list.

Approving a session request

Depending on how the Security Policy Administrator configured the policy, a sessions request will either require approval by one or more SPP users, or be auto-approved.

You can configure SPP to notify you of an access request that requires your approval. For more information, see Configuring alerts on page 95.

To approve or deny a session request

Click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see. You can select columns including:

- **Action**: Displays **Approve only this request** and **Deny only this request**.
- **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).
- **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, **API Key**, or **Telnet**).
- **Account**: Displays the managed account name.
- **Ticket Number**: Displays the ticket number, if required.
- **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).

- **Search**: For more information, see Search box on page 78.

Launching the SSH client

Once an SSH session request becomes available, the requester can launch the SSH client to start the session.

To launch the SSH client to begin your session then close your session

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Hostname Connection String) required to launch the SSH client.
2. Click the ▶ **Start SSH Session** button associated with the asset name. In the web client, a session will launch if you have an application registered (`ssh://` for SSH protocol).

   NOTE: The ▶ **Start SSH Session** options are available only if enabled by user preferences.
3. In the SSH client, run the commands or programs on the target host.

   If there is no activity in an open session for about 10 minutes, the session will be closed. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.
4. Once you are completed, log out of the target host and select ✓ **Check in** to complete the session request process.

Launching an RDP session

Once an RDP session request becomes available, the requester can launch the remote desktop connection to start the session.

To launch a remote desktop connection

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Username Connection String) required to launch the remote desktop session.
2. In the web client:

   NOTE: The ▶**Start RDP Session** option is available only if enabled by user preferences.

   - If you have an application registered (`rdp://` for RDP sessions), you can click the ▶ **Start RDP Session** button associated with the asset name then click **Connect**. See KB 313918 for details on application registration. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.
   - If you do not have an application registered, download the RDP launch file instead of using the ▶ **Start RDP Session** button. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.

Begin your RDP session and close the session

1. In the remote desktop session, run the commands or programs on the target host. If there is no activity in an open session for about 10 minutes, the session will be closed. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.
2. Once you are completed, log out of the target host and select ✓ **Check in** to complete the session request process.

Configuring and launching a Remote Desktop Application session

In order to launch a remote desktop application session request, some additional configuration is required.

To configure and launch a remote desktop application

1. Install and configure Safeguard for Privileged Sessions's RemoteApp launcher available starting with 6.12. For more information, see One Identity Safeguard for Privileged Sessions Administration Guide.
2. Publish the **OISGRemoteAppLauncher** application following Microsoft's instructions. All remote applications that will be launched using SPP/SPS need to be configured to launch with the OISGRemoteAppLauncher and include a command line which references the intended remote application. Take note of the **RemoteApp Program Name** and **Alias** since they will be needed when configuring the access request policy.

3. On **Asset Management** > **Assets**, you need the following assets (for more information, see Adding an asset):
   a. **Windows Server** asset: This asset will be used to connect with a Windows Application Server.
   b. **Other**/**Other Managed** asset: This asset (of either platform type) is used to connect with the remote application. It requires the following settings:
      - **Network Address**: None
      - **Authentication Type**: None
      - An account from the remote application added to the **Accounts** tab.
4. On **Security Policy Management** > **Entitlements**, you will need an entitlement containing a Remote Desktop Application access request policy. For more information, see Creating an access request policy.
5. Within Safeguard for Privileged Sessions, a channel policy needs to be modified or created to include the following attributes. This channel policy will also need to be referenced from an RDP connection policy. For more information, see One Identity Safeguard for Privileged Sessions Administration Guide.
   a. In **RDP Control** > **Connections**, set the **Channel policy** to **applications**.
   b. In **RDP Control** > **Channel Policies**, create the following:
      i. **Dynamic virtual channel**: No configured settings.
      ii. **Custom**: Add the following to **Permitted channels**:
         - `rail`
         - `rail_ri`
         - `rail_wi`

Once a remote desktop application session request becomes available, the requester can launch the remote desktop connection to start the session.

To launch a remote desktop application connection

In the web client: Click the ▶**Start RDP Session** button associated with the asset.

NOTE: The ▶**Start RDP Session** option is available only if enabled by user preferences and if you have installed Session Client Application Launch Uri System (for more information, see SCALUS).

NOTE: A black window may appear on the screen as the launcher loads the remote desktop application session.

Reviewing a session request

The Security Policy Administrator can configure an access request policy to require a review of completed session requests for assets or accounts in the scope of the policy.

NOTE: You can configure SPP to notify you of an access request that requires your review. For more information, see Configuring alerts on page 95.

Desktop Player User Guide

To download the player user guide, go to One Identity Safeguard for Privileged Sessions - Technical Documentation. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.

To review a completed sessions request

Select **Reviews** on the left of the page to manage reviews. On the **Reviews** page, you can:

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click **Mark all the selected requests as reviewed**.
  - If a comment is needed, this icon will display as **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
  - **Action**: Displays **This request requires review comments** or **Mark only this request as reviewed**.
  - **Requester**: Displays the user name of the requester.
  - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, **API Key**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.
  - **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 78.

Appliance Management

In the web client, expand the **Appliance Management** section in the left navigation pane. Settings are available to Appliance Administrators, Operations Administrators, and the Bootstrap Administrator (Auditors have read-only access).

Appliance

Use the Appliance settings to view general information about the appliance, run diagnostic tools, and reset or update the One Identity Safeguard for Privileged Passwords hardware appliance.

SPP can be set up to use a virtual appliance. For more information, see Using the virtual appliance and web management console on page 50.

web client: Navigate to **Appliance Management** > **Appliance**.

One Identity Safeguard for Privileged Passwordsprovides the following information to help you resolve many common problems you may encounter as you deploy and use your appliance.

Table 15: Appliance settings

Setting	Description
Appliance Diagnostics	Where you execute a trusted, secure diagnostics package to help solve a configuration issue, synchronization issue, clustering issue, or other internal issues.
Appliance Information	Where you view general information about the appliance, as well as its performance utilization and the memory usage. You can also edit the Appliance Name and Host DNS Suffix.
Debug	Where you enable or disable debug logging to a syslog server.
Licensing settings	Where you add or update a SPP license.
Network Diagnostics	Where you run diagnostic tests on your appliance.

Setting	Description
Networking	Where you view and configure the primary network interface, and if applicable, the sessions network interface.
Operating System Licensing	Available on virtual machine only. Not available on hardware. Where you configure the operating system for the virtual appliance.
Patch Updates	Where you upload and install a patch update file.
Power	Where you shut down or restart your appliance in the web client.
SSH Algorithms	Where you configure SSH Algorithms to manage account passwords and SSH keys.
Support bundle	Where you create a support bundle containing system and configuration information to send to One Identity Support to analyze and diagnose issues with your appliance.
Time	Where you enable Network Time Protocol (NTP) and set the primary and secondary NTP servers. A replica in the cluster will always reference the primary appliance as its NTP server. You can also manually set the time on a primary but not a cluster. **CAUTION: Manually setting the time should be done with caution. Time changes can cause critical data loss.**
Factory Reset	Available on hardware only. Not available on a virtual machine. Where you perform a factory reset to revert your appliance to its original state when it first came from the factory.
Lights Out Management (BMC)	Available on hardware only. Not available on a virtual machine. Where you enable and disable lights out management, which allows you to remotely manage the power state and serial console to SPP using the baseboard management controller (BMC).

In addition to the appliance options, One Identity Safeguard for Privileged Passwords provides these troubleshooting tools:

Table 16: Additional troubleshooting tools

Tool	Description
Activity Center	View the details of specific events or user activity. For more information, see Activity Center on page 564.
LCD status messages	Use the LCD screen on the appliance to view the status of the appliance as it is starting up or shutting down. For more information, see LCD status messages on page 642.

Tool	Description
Recovery Kiosk (Serial Kiosk)	A terminal or laptop connected directly to the appliance to view basic appliance information, restart the appliance remotely, shut down the appliance, reset the bootstrap administrator's password to its initial value, perform a factory rest, or to generate and send a support bundle to a Windows share. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.

Appliance Diagnostics

Appliance Administrators can execute a trusted, secure appliance diagnostics package to help solve issues with configuration, synchronization, and clustering, as well as other other internal challenges. The appliance diagnostics package is available from the web Support Kiosk, not the Serial Kiosk (Recovery Kiosk). The appliance diagnostics package can be used even when the appliance is in quarantine. To protect against external threats, Safeguard rejects illegitimate appliance diagnostics packages. The manifest file in the appliance diagnostics package lists criteria that may include the minimum Safeguard version, appliance ID, and expiration time-stamp UTC. New product code and database changes are not included in an appliance diagnostics package.

web client: Navigate to **Appliance** > **Appliance Diagnostics**.

1. The state of the appliance displays (for example, **Online**). Click **Refresh** to update the state.
2. If no appliance diagnostics package has been loaded, click **Upload Diagnostics**, select the appliance diagnostics package file that has an .sgd extension, then click **Open**.
   - If the upload criteria is not met, the appliance diagnostics package is not uploaded and a message like the following displays: `The minimum Safeguard version needed to run this diagnostic package is <version>.`
   - If the upload is successful, the **Diagnostic Package Information** displays with the **Status** of **Staged**. You can:
     - Select **Execute** and wait until the **Status** changes to **Completed** or **Error**.
     - Select **Remove** to delete the appliance diagnostics package and the associated log file.
3. Once uploaded, you can perform these activities.
   - If the **Expiration Date** has not passed, you can select **Execute** to execute the appliance diagnostics package again.
   - Select **Delete** to delete the appliance diagnostics package, the associated log file, and stop any appliance diagnostics package that is running. Before uploading a different appliance diagnostics package, you must delete the

current one because there can be only one appliance diagnostics package per appliance.

- Select **Download Log** to save the log file. Audit log entries are available through the Activity Center during and after execution and are part of the appliance history. A log is also available during and after execution until the diagnostic package has been deleted.

Appliance Information

It is the responsibility of the Operations Administrator or the Appliance Administrator to monitor the status of the appliance.

To go to **Appliance Information**:

- web client: Navigate to **Appliance** > **Appliance Information**.

To refresh:

- web client: Select the number of seconds to refresh in **Refresh every 30 seconds** . A refresh is started immediately when the value is changed and the next refresh is scheduled based on the selected value.

The following information displays.

Table 17: Appliance properties

Property	Description
Appliance Name	The name of the appliance. The Appliance Administrator can modify the name. Click **Edit** to enable the **Appliance Name** text box. Enter a new appliance name and click **Save**.
Host DNS Suffix	The host DNS suffix name. The Appliance Administrator can modify the name. Click **Edit** to enable the **Host DNS Suffix** text box. Enter a new name and click **Save**.
Host	The appliance network server IP address.
Appliance Version	The version of the SPP Appliance.
Uptime	The amount of time (hours and minutes) the appliance has been running.
Last Boot Date	The last date the appliance was booted up.

General tab information

Disk is a graphical display of the amount of used and free disk space. When the disk usage is over 80%, the log reflects: `DiskUsageWarningEvent`.

Table 18: General tab

Property	Description
Manufacturer	The system manufacturer.
Model	The system model.
Bios Description	The system bios description.
Bios Serial Number	The system's bios serial number.
Serial Number	The media access control address (MAC address) assigned to the network interface for communications.
Ship Date	The appliance ship date.
Processor	The processor information.
Virtual Memory	The virtual memory allocation.
Physical Memory	The physical memory allocation.
TLS 1.2 only	Click this toggle to disable earlier versions of the Transport Layer Security (TLS) protocol and use only TLS v1.2. NOTE: You must reboot your appliance after enabling **TLS 1.2 only**. web client: enabled and disabled

Performance tab

Table 19: Performance tab

Property	Description
Total CPU and **Core_n**	Displays the CPU information and the performance utilization of your appliance.
Memory	Displays the memory usage of your appliance; what is currently in use and what is free.
Disk Space	Displays the disk space used and free.

Shutting down the appliance

You can power down an appliance from the web client or directly from the appliance itself.

> **CAUTION: Rebooting the appliance causes a service outage for any current users.**

To shut down an appliance

You can shut down your appliance from the web client via **Appliance** > **Power**. For more information, see Power on page 147.

Appliance: Shut down from the appliance

You can use the **Red X** button on the front panel of the appliance to shut it down. Press and hold the **Red X** button for four seconds until it displays `POWER OFF`.

> **CAUTION: Once the Safeguard appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.**

Restarting the appliance

You can restart an appliance from the web client or directly from the appliance itself.

To restart an appliance

You can restart your appliance from the web client via **Appliance** > **Power**. For more information, see Power on page 147.

Appliance: Restart from the appliance

After the appliance powers off, you will need physical access to start it. Press the **Green check mark** button on the front panel of the appliance for NO MORE than one second to power on the appliance.

> **CAUTION: Once the Safeguard appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.**

Setting the appliance name and Host DNS Suffix

SPP automatically assigns a name to the appliance; however, you can change the name from the **Appliance Information** page. In the web client, you can also edit the Host DNS Suffix that was set during the initial setup of SPP.

To edit the appliance name and host DNS suffix

1. Go to the page:
   - web client: Navigate to **Appliance** > **Appliance Information**.
2. To the right of the **Appliance Name** and **Host DNS Suffix**, click **Edit** to enable both fields for editing.
3. Make any changes required to the **Appliance Name** or **Host DNS Suffix**.
4. Click **Save**.

Debug

For each SPP internal service, you can specify the level of logging and the external syslog server for storing debug logs. This allows for debugging in real time.

Debug logging is appliance specific. The data sent to the syslog server can include but is not limited to Support Bundle debug data. Cluster wide TLS audit event can be logged to a syslog server (see Syslog Events).

Debug logging is off by default but you can turn it on or off. Because debug logs can be sizable, you may want to turn it on for debugging a specific scenario or testing and turn it off for daily operations.

Using the API to control TLS log connection messages

Using the API, you can control if TLS log connection messages are generated to the debug logs when the TLS connection to an external server is closed. If the log level is set (see below), the event is also sent to the syslog server.

To log TLS connection information, set the `NetworkDebugEnabled` property from the `https://<network address>/service/appliance/v4/Service/Debug` endpoint to true. For more information, see Using the API on page 44.

To configure debug logs to send to a syslog server

1. You will need a configured syslog server. If you have not configured a syslog server, you will see a message like this: `To configure additional debut logging options, you need to configure a syslog server.` Click **Configure a syslog server**. For more information, see Configuring and verifying a syslog server on page 234.
2. If you have a syslog server configured, navigate to **Appliance** > **Debug**.
3. Select a **Syslog Server** to which you want to send debug logs. The default is **Do not log to syslog**.
4. In **Facility**, select which syslog facility to which you want to use: **Kernel**, **User**, **Mail**, **Daemons**, **Authorization**, or **Syslog**.
5. Set the log level.

- To set all log levels, click **Set All** then choose to **Set All** at one of the levels. This is useful to set the most common level of logging you want for most services.
- To set an individual **Service Name**'s log level, select next to the service to change the log level for that service.

When you select from either the set all levels or the individual service name level, the log includes the log level selected as well as those listed below the level you selected. The information is immediately sent to the server. For example:

- Debug (includes Debug, Information, Warning, and Error)
- Information (includes Information, Warning, and Error)
- Warning (includes Warning and Error)
- Error (includes only Error)
- None (Disabled): No logs are sent

6. The grid displays each **Service Name (enum name)** that supports debug logging and the current **Log Level**.
   - Click **Refresh** at any time to display the latest information.
   - Click **Search** to locate a specific service.

Licensing settings

CAUTION: All customers upgrading to SPP 7.0 require a new license. For more information, contact Support.

It is the responsibility of the Appliance Administrator to manage the Safeguard for Privileged Passwords licenses.

Hardware appliance

The One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance ship with the Privileged Passwords module which requires a valid license to enable functionality.

You must install a valid license. Once the module is installed, SPP shows a license state of **Licensed** and is operational. If the module license is not installed, you have limited functionality. That is, even though you will be able to configure access requests, if a Privileged Passwords module license is not installed, you will not be able to request a password release.

Virtual appliance Microsoft Windows licensing

You must license the virtual appliance with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed

to your Sales Representative. The virtual appliance will not function unless the operating system is properly licensed.

Licensing setup and update

To enter licensing information when you first log in

The first time you log in as the Appliance Administrator, you are prompted to add a license. The **Success** dialog displays when the license is added.

On the virtual appliance, the license is added as part of Initial Setup. For more information, see Setting up the virtual appliance on page 52.

> IMPORTANT: After successfully adding a license, the Software Transaction Agreement will be displayed and must be read and accepted in order to use SPP.

To configure reminders for license expiration

To avoid disruptions in the use of SPP, the Appliance Administrator must configure the SMTP server, and define email templates for the `License Expired` and the `License Expiring Soon` event types. This ensures you will be notified of an approaching expiration date. For more information, see Enabling email notifications on page 219.

Users are instructed to contact their Appliance Administrator if they get an "appliance is unlicensed" notification.

As an Appliance Administrator, if you receive a "license expiring" notification, apply a new license.

To update the licensing file

Safeguard licenses can be updated both on hardware and virtual machines, whereas OS licenses can be updated only on virtual machines.

To perform licensing activities

Navigate to **Appliance Management** > **Appliance** > **Licensing**.

- To upload a new license file, click **+ Upload new license file** and browse to select the current license file. The Software Transaction Agreement will also be displayed during this process and must be read and accepted in order to complete the licensing process.
- To remove the license file, select the license and click **Remove selected license**.
- To get more information on the license and to export license data, click the **What do these numbers mean?** button, or click on the numbers in the tile.

  If you want to export data about users, desktops or systems in CSV or JSON format, navigate to the table from which you want to export data by clicking the corresponding tab, for example **Users Used**.

  Click the export icon located on the table. For more information on exporting, see Exporting data.

  Below is the list of the available tabs.

  For device-based licenses:

    - General
    - Desktops Used
    - Other Desktops
    - Systems Used
    - Other Systems
    - History

  For user-based licenses:

    - General
    - Users Used
    - Password Vault Only
    - Other Users
    - History

- The **General** tab, contains general information about the license:
    - License usage and consumption
    - Counts of all managed and unmanaged components
    - How licenses are counted
    - License Number
    - License Type
    - Expiration Date
    - Product Version
    - Date Added
    - Added By

Factory Reset

As an Appliance Administrator, you can use the Factory Reset feature to reset a SPP Appliance to recover from major problems or to clear the data and configuration settings on the appliance.

Factory reset is not an option for virtual appliances. You will need to redeploy the appliance.

CAUTION: Care should be taken when performing a factory reset against a physical appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. Performing a factory reset will NOT reset the BMC/IPMI interface or the IP address. However, the BMC/IPMI interface will need to be reenabled after the reset has completed (for more information, see Lights Out Management (BMC)). The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

The appliance resets to the current Long Term Support (LTS) version. For example, if the appliance is running version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, the appliance will reset down to 6.0 LTS and you will have to patch up to your desired version. For more information, see Long Term Support (LTS) and Feature Releases on page 42.

Factory reset on a clustered appliance

Performing a factory reset on a clustered hardware appliance will not automatically remove the appliance from a cluster. The recommended best practice is to unjoin an appliance from the cluster before performing a factory reset on the appliance. After the unjoin and factory reset, the appliance must be configured again. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.

To perform a factory reset from the web client

1. Go to Factory Reset on hardware (not virtual machine):
   - Navigate to **Appliance Management** > **Appliance** > **Factory Reset**.
2. Click **Factory Reset**.
3. In the Factory Reset confirmation dialog, enter the words **Factory Reset** and click **Factory Reset**.

   The appliance will go into Maintenance mode to revert the appliance. If the appliance was in a cluster, you may need to unjoin the factory reset appliance. The factory reset appliance must be configured again. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69. In addition, when you log in to the appliance, you will be prompted to add your SPP licenses.

You can also perform a factory reset from the Recovery Kiosk or Support Kiosk. For more information, see Performing a factory reset on page 595.

Lights Out Management (BMC)

The Lights Out Management feature allows you to remotely manage the power state and serial console to Safeguard for Privileged Passwords using the baseboard management controller (BMC). When a LAN interface is configured, this allows the Appliance Administrator to power on an appliance remotely or to interact with the Recovery Kiosk.

The Appliance Administrator can enable and configure the Lights Out Management feature. When Lights Out Management is enabled, the Appliance Administrator can set or change the password and modify the network information for the baseboard management console (BMC). When disabled, SPP immediately resets the password to a random value and resets the network settings to default values.

Lights Out Management is only available using hardware (not a virtual machine):

- Use the virtual appliance Support Kiosk, **Lights Out Managment (BMC)**. For more information, see Support Kiosk on page 56.

LAN interface required

This feature requires a LAN interface to be enabled and configured. One Identity Safeguard for Privileged Passwords's BMC supports the following LAN interfaces to provide this functionality:

- SSH
- IPMI v2
- Web
- Serial over Lan

It is strongly recommended that the LAN interface only be enabled in trusted environments.

To enable Lights Out Management

A static IP address will need to be assigned and a network cable will need to be connected to the IPMI ethernet port on the back of the appliance. This is in addition to the standard X0 network interface.

1. Navigate to **Lights Out Management (BMC)**.
2. Click the **Enable Lights Out Management** toggle to enable or disable this feature. Set toggle on or toggle off.
3. Once enabled, enter the following information about the BMC:
   a. **IP address**: The IPv4 address of the host machine.
   b. **Netmask**: The network mask IPv4 address.
   c. **Default Gateway**: The default gateway IPv4 address.
4. Use **Set BMC Admin Password** to set the password for the host machine.

   Maximum password length: 20 characters.

> NOTE: If this feature was previously enabled, you will see an **Update BMC Admin Password** button instead. Optionally, click the **Update BMC Admin Password** button to reset the password for the host machine.

5. Click **OK** to save the settings on the host machine.

Accessing the BMC

Once Lights Out Management is enabled in SPP, you can access the BMC via:

- SSH to connect to the IPMI port to remotely manage the power state and serial console to SPP
- Web browser

SSH connection

The SPP Kiosk Console can be accessed via Putty, Linux command line, or your preferred SSH Client.

1. Connect to the IP assigned to the IPMI interface and login with the Admin user. (Default credentials are ADMIN/admin)
2. At the prompt run: `start /system1/sol1`. There may be a delay. Please wait for the connection. A message like the following gives you the instructions to proceed:
```
->start /system1/sol1
press <Enter>, <Esc>, and then <T> to terminate session
(press the keys in sequence, one after the other)
```
3. On the menu shown below, navigate using the arrow keys. Press the right arrow to select a menu option, press the left arrow to return to the menu list, press up or down to select a different menu option.

   `Appliance Information >`

   `Power Options >`

   `Backups >`

   `Admin Password Reset >`

   `Factory Reset >`

   `Support Bundle >`
4. If the screen freezes, or displays distorted information, you can press **CTRL+R** or **CTRL+D** to refresh the screen.
5. To exit the Kiosk press **Enter**, then press **ESC**, then press **SHIFT+T**. At the prompt, type in `exit`.

If the appliance is in Quarantine, please generate a Quarantine Bundle from the Kiosk menu and copy the file to a network share. After the bundle is retrieved, perform a Reboot via the Kiosk, to see if the appliance will recover on its own. If it remains in Quarantine, a Factory Reset will likely be necessary. For more information, see Performing a factory reset on page 595.

Web browser interface

If you experience difficulty logging in through SSH, web access is also available.

1. In your browser, go to the IP address of your IPMI interface. (that is, `https://10.10.10.10`), and login with your BMC admin account. The default is ADMIN/admin.
2. You can attempt to fix the SSH connection, by navigating to **Maintenance > Unit Reset > Select Reset**. After 60 seconds re-attempt the SSH connection.
3. Login to the Kiosk via the web by navigating to **Remote Control > Select Launch SOL**. (Java is required for this method, the Kiosk will launch in a JNLP window.)
4. Use the cursor keys and return to navigate. **Page Up** is used for backspace. It is not possible to copy and paste when using the Java viewer.

Rebooting

A reboot from the BMC web browser interface is only a hardware level reboot.

If you need to reboot using the web browser interface:

1. Log into the BMC web browser interface.
2. Open the Serial over Lan emulator, which opens the Kiosk interface.
3. Select reboot from the menu.

See KB 263835: How to remotely access the Kiosk via the Lights Out Management / BMC / IPMI interface.

Network Diagnostics

SPP makes these diagnostic tests available for the Appliance Administrator and Operations Administrator.

NOTE: When you run these diagnostic tests, they are run on the appliance.

1. Go to Network Diagnostics:
   - web client: Navigate to **Appliance** > **Network Diagnostics**.
2. Choose the type of test to perform and complete the steps.
   - ARP: Use Address Resolution Protocol (ARP) to discover the Interface, Internet Address, Physical Address, and Type (dynamic or static).
   - Netstat: Use netstat to display the active connection protocol, local address, foreign address, and state.
   - NS Lookup: To obtain your domain name or IP address.
   - Ping: To verify your network connectivity and response time.
   - Show Routes: To retrieve routing table information.
   - Telnet: To access remote computers over TCP/IP networks like the internet.
   - Throughput: Test throughput to other appliances in the cluster.

- Trace Route: To obtain your router information; trace route determines the paths packets take from one IP address to another.

ARP

Use Address Resolution Protocol (ARP) to discover the Interface, Internet Address, Physical Address, and Type (dynamic or static).

1. Navigate to **Appliance** > **Network Diagnostics**.
2. Click **ARP**.
3. Click **Display ARP Table** to run the test. The test results display in the **Output** window and may include the **Interface**, **Internet Address**, **Physical Address**, and **Type**.

Netstat

Use netstat to display the active connection protocol, local address, foreign address, and state.

1. Navigate to **Appliance** > **Network Diagnostics**.
2. Click **Netstat**.
3. Click **Display Connections** to run the test. The test results display in the **Output** window and may include the **Active Connections**, **Protocols**, **Local Address**, **Foreign Address**, and **State**.

NS Lookup

Use the NS Lookup query to obtain the domain name server or IP address of the specified host in relation to the SPP Appliance.

1. Navigate to Network Diagnostics:
   - web client: Navigate to **Appliance** > **Network Diagnostics**.
2. Click **NS Lookup**.
3. Enter the remote host's **IP address or Hostname**.
4. In **Record Type**, select the type of DNS record to be queried.
5. Select **More Settings** then, in **Query Options**, select the type of query.
6. Click **Lookup** to run the test. The test results display in the **Output** window.

Ping

Use the ping test to verify network connectivity and response time between the SPP Appliance and the specified host.

1. Navigate to Network Diagnostics:
   - web client: Navigate to **Appliance** > **Network Diagnostics**.
2. Click **Ping**.
3. Enter the remote host's **IP or Hostname**.
4. Optionally, click **More Settings** then configure these additional settings:
   - **Resolve IP addresses to hostnames**
   - **Size**: Buffer size; range from 1 to 65500
   - **Time to live**: Enter a value from 1 to 255
   - **Record route for count hops (IPv4 only)**: Enter a value from 1 to 9
   - **Timeout in milliseconds to wait for each reply**: Enter a value from 1 to 4000
   - **Number of echo requests to send**: Enter a value from 1 to 65527
   - **Set "don't fragment" flag in packet (IPv4 only)**
   - **Type of service**: Enter from 1 to 255
   - **Time stamp for count hops (IPv4 only)**: Enter from 1 to 4
   - **Use internal address as source**
5. Click **Ping** to run the test. The test results display in the **Output** window.

Show Routes

Use Show Routes to retrieve routing tables to further investigate connectivity issues.

1. Navigate to Network Diagnostics:
   - web client: Navigate to **Appliance** > **Network Diagnostics**.
2. Select **Show Routes**.
3. Click **Show Routes** to run the test.
4. The test results display in the **Output** window.

Telnet

Use telnet to test TCP/IP connectivity between the SPP Appliance and the specified host.

1. Navigate to Network Diagnostics:
    - web client: Navigate to **Appliance** > **Network Diagnostics**.
2. Click **Telnet**.
3. Enter the remote host's **IP or Hostname**.
4. Enter the **Port** number on a target host. The default is 23 and you can enter a value from 0 to 65535.
5. Optionally, click **More Settings** to configure the **Connection Timeout** from 1 to 15 seconds.
6. Click **Connect** to run the test. The test results display in the **Output** window.

Throughput

Test throughput to other appliances in the cluster.

1. Navigate to **Appliance** > **Network Diagnostics**.
2. Click **Throughput**.
3. In **Target Appliance**, select the target cluster appliance from the list.
4. In **MB to Transfer**, select the size of the transfer to test (1 to 1000 MB).
5. Click **Test Throughput** to run the test. View the **Output**.

Trace Route

Use the Trace Route test to obtain route information, such as the paths packets take from one IP address to another.

1. Navigate to Network Diagnostics:
    - web client: Navigate to **Appliance** > **Network Diagnostics**.
2. Click **Trace Route**.
3. Enter the remote host's **IP or Hostname**.
4. Optionally, click **More Settings** to configure the following:
    - **Resolve IP addresses to hostname**
    - **Maximize number of hops to search for target**
    - **Timeout in milliseconds to wait for each reply**
5. Click **Trace** to run the test. The test results display in the **Output** window.

Networking

On **Networking**, view and configure the primary network interface, and if applicable, a proxy server to relay web traffic, and the sessions network interface.

The Network Interface (X1) can be used to add additional virtual network adapters associated with X1 in the web client.

It is the responsibility of the Appliance Administrator to ensure the network interfaces are configured correctly.

> **CAUTION: For AWS or Azure, network settings user interfaces are read-only. Network settings configured by the AWS or Azure Administrator. Changing the internal network address on a clustered appliance will break the cluster and require the appliance to be unjoined/rejoined.**

To modify the networking configuration settings

1. Navigate to **Appliance** > **Networking**.
2. For **Network X0**, complete the network settings below. For more information, see Modifying the IP address on page 143.
   - **MAC Address**: (Read-Only) The media access control address (MAC address), a unique identifier assigned to the network interface for communications.
   - **IPv4 Address**: The IPv4 address of the network interface.
   - **IPv4 Subnet Mask**: The IPv4 subnet mask of the network interface.
   - **IPv4 Gateway**: The IPv4 default gateway.
   - **DNS Servers**: The IP address for the primary DNS servers.
   - **DNS Suffixes**: The network suffixes for the DNS servers.

     NOTE: You can also use the **Global DNS Suffixes** field on the **Appliance** > **Networking page**.
   - **IP6 Address**: The IPv6 address of the network interface.
   - **IPv6 Prefix Length**: The IPv6 subnet prefix length which is range-validated. Valid values are 1 through 127 when an IPv6 address is present.
   - **IPv6 Gateway**: The IPv6 default gateway.
3. For **Network X1** (web client), complete the network settings below to add additional virtual network adapters on up to 31 VLANs.
   - **MAC Address**: (Read-Only) The media access control address (MAC address), a unique identifier assigned to the network interface for communications.
   - **IPv4 Address**: The IPv4 address of the network interface.
   - **IPv4 Subnet Mask**: The IPv4 subnet mask of the network interface.
   - **IPv4 Gateway**: The IPv4 default gateway.
   - **DNS Servers**: The IP address for the primary DNS servers.

- **DNS Suffixes**: The network suffixes for the DNS servers.

  NOTE: You can also use the **Global DNS Suffixes** field on the **Appliance** > **Networking page**.
- **IP6 Address**: The IPv6 address of the network interface.
- **IPv6 Prefix Length**: The IPv6 subnet prefix length which is range-validated. Valid values are 1 through 127 when an IPv6 address is present.
- **IPv6 Gateway**: The IPv6 default gateway.
- **VLAN ID**: The VLAN ID for the network. This is only applicable to network interfaces added by the administrator. Changes to this field will also update the name of the adapter.

4. For the **Proxy Server** (web client), complete the network settings below.
   - **Proxy URI**: The IP address or DNS name of the proxy server.
   - **Port**: The port number used by the proxy server to listen for HTTP requests. The value is an integer from 1 to 65535. If different ports are specified in the proxy URI and the **Port** field, the **Port** field takes precedence.
   - **Username**: The user name used to connect to the proxy server. The username and password are only required if your proxy server requires them to be specified.
   - **Password**: The password required to connect to the proxy server. The username and password are only required if your proxy server requires them to be specified.
5. Click **Show Static Routes** and make changes using the information which follows. When you are done, click **Save**. When you click **Save**, a message like the following displays: `Changing these values may cause all users to lose connection to the appliance`. This is a general `Saving network settings error` and not specific to static routes.
   - Use the following toolbar buttons, as needed.
     - To add a route, click + and complete the information.
     - To modify the information for a route, select the route, click **Edit**, and then change the information.
     - To delete a route, select the route then click **Delete Static Route**. The route is immediately deleted.
     - To discard unsaved changes and revert to what was last retrieved from the database, select the route and click **Revert all unsaved Static Route edits**.
   - The following information can be added or changed:
     - **IP Version**: Select IPv4 or IPv6.
     - **Prefix**: The IPv4 or IPv6 IP address.
     - **Prefix Length**: The IP subnet prefix length.

- **Next Hop**: The IP address of the next closest or most optimal router in the routing path.
- **Metric**: A value that identifies the cost that is associated with using the route.

Modifying the IP address

You can change the IP address of an SPP Appliance as long as the other appliances in the SPP cluster are able to see the new subnet.

It is recommended you use the procedure below in a test environment and then deploy the steps in production. Allow plenty of time for the IP address to change. The operation will take several minutes to complete before the cluster has adjusted to the change.

1. Ensure you are using SPP 2.4 or above.
2. Before changing the X0 IP address, make a backup.
3. Generate a support bundle on the appliance you plan to modify the IP address on. Start with the replica first.
4. After the X0 IP address change, verify clustering is working. It is recommended you change some data on the primary and verify it appears on the replica by logging on to the replica.
5. Repeat step 3, 4, and 5 for the other replicas.
6. Once the replicas are changed, proceed with the Primary.

Safeguard for Privileged Sessions IP address change

CAUTION: When SPP (SPP) and Safeguard for Privileged Sessions (SPS) are linked and then the IP address of either the Safeguard for Privileged Sessions cluster master (Central Management role) or the SPP primary appliance are changed, then the SPP/SPS link will need to be redone. See the information that follows.

1. Use the following information in the Safeguard for Privileged Sessions documentation to understand Safeguard for Privileged Sessions cluster roles, settings, and IP address updating.
   - Cluster roles: Assigning roles to nodes.
   - Network settings: Setting Safeguard for Privileged Sessions network interface and naming settings, including IP addresses.
   - Building a cluster: Assigning the Central Management node in a cluster (which cannot be undone) and then link other nodes.
   - Assigning roles to nodes in your cluster: Assigning roles, including the Central Management role, to nodes in a cluster.
   - Updating the IP address of a node in a cluster: Updating the IP address of Safeguard for Privileged Sessions Managed Nodes.

- Managing a High Availability One Identity Safeguard for Privileged Sessions (SPS) cluster: Setting up Safeguard for Privileged Sessions to handle nodes if the primary node stops functioning.

2. If the IP address is changed, you must relink the cluster. For more information, see Linking SPS to SPP.
3. Once the Safeguard for Privileged Sessions IP addresses are successfully changed, you will need to delete the session connection in the SPP settings and relink the Safeguard for Privileged Sessions cluster master to the SPP primary. For more information, see SPP and Safeguard for Privileged Sessions appliance link guidance on page 684.

Operating System Licensing

Available on virtual machine only not via hardware.

It is the responsibility of the Appliance Administrator to ensure the operating system is configured. Operating system licensing is automatic in the AWS and Azure deployments.

Use the **Operating System Licensing** pane to view and configure the operating system of a virtual appliance.

1. Navigate to Operating System Licensing:
   - web client: Navigate to **Appliance** > **Operating System Licensing**.
2. Click **Refresh** anytime to refresh the settings.
3. The display shows if **Windows is licensed with** KMS or licensed with a product key. Click **Details** to see additional information.

SSH Algorithms

The Appliance Administrator has the option to configure SSH Algorithms, if necessary, to restrict the algorithms used when connecting to any SSH server. The settings are applied whenever Safeguard for Privileged Passwords connects to any SSH server, either to connect to an asset using SSH or to connect to an archive server using SSH.

When an SSH client connects to a server, each side of the connection offers four lists of algorithms to use as connection parameters to the other side. These are:

- Public Key: The public key algorithms accepted for an SSH server to authenticate itself to an SSH client
- Cipher: The ciphers to encrypt the connection
- Kex: The key exchange methods that are used to generate per-connection keys
- MAC: The message authentication codes used to detect traffic modification

By default, Safeguard for Privileged Passwords offers all supported algorithms when using SSH to connect to an archive server or asset. For each algorithm type, you can configure Safeguard to offer a subset of the supported algorithms. To return to the default (support all algorithms), delete all algorithm information entered then save the changes.

For a successful connection, there must be at least one mutually-supported choice for each parameter. Safeguard for Privileged Passwords may initiate an SSH connection to an asset or archive server and not be able to negotiate a mutually-acceptable algorithm. An error is reported and an attempt is made to identify the algorithm type that could not be negotiated. Some SSH servers do not provide enough information to identify the algorithm type.

To identify SSH algorithms

1. Navigate to SSH Algorithms:
   - web client: Navigate to **Appliance** > **SSH Algorithms**.
2. Click **Refresh** anytime to refresh the settings.
3. Enter a comma separated list of the algorithms you want in the text boxes. Leave the text box blank to allow all supported algorithms.
   - **Public Key**
   - **Cipher**
   - **Kex**
   - **Mac**
4. Click **Save**.

Adjusting the preferred order of preference for public key algorithms

By default, the list of public key algorithms supported for host keys and available for identity keys is negotiated with the SSHD server in this order of preference:

1. Ssh-ed25519,
2. ecdsa-sha2-nistp256,
3. ecdsa-sha2-nistp384,
4. ecdsa-sha2-nistp521
5. ssh-rsa
6. rsa-sha2-256
7. rsa-sha2-512
8. ssh-dss

You can change the preferred order and/or restrict the available algorithms to a subset of this list by configuring the PublicKey list using the SshAlgorithms API.

Patch Updates

It is the responsibility of the Appliance Administrator to update or upgrade One Identity Safeguard for Privileged Passwords by installing an update file to modify the software or configuration of the running appliance. See the Download Software page for available SPP releases and version patches.

If an update fails, the audit log reflects: `PatchUploadFailed`.

Clustered environment

Apply the patch so all appliances in the cluster are on the same version. For more information, see Patching cluster members.

To install an update file

IMPORTANT: Once you start a patch update, do not leave or refresh the page. Doing so will cause the browser to lose track of the patch update and you will have to restart the process.

1. Back up your system before you install an update file. For more information, see Backup and Restore on page 161.
2. Go to Patch Updates:
   - web client: Navigate to **Appliance** > **Patch Updates**.
3. The current **Appliance Version** displays along with the operating system level, whether the appliance is online or offline, and whether the appliance is the Primary.
4. Click **Upload a File** and browse to select an update file. Simply uploading a file does not install the file. You must complete the next step.

   If the patch verification fails an error alert displays, click on any of the Error or Warning counts to view the errors or warnings currently logged.
5. Once the file has successfully uploaded, click one of the following:
   - **Install Now** to install the update file. Respond to the confirmation dialog which includes any warnings. The install process begins and the appliance goes into maintenance mode.
     Once you install an update file, you cannot uninstall it. This button is disabled until the patch is distributed to all cluster members. If this is a single-appliance cluster distribution is not required.
   - **Distribute to Cluster** is disabled if there are errors. Click **Distribute to Cluster** to initiate the distribution of the patch to all cluster members. Clicking **Cancel** will stop distribution. Cluster Update Status blocks will be updated as each member receives the patch
   - **Check Errors** to initiate a check of pre-patch conditions. If the patch has not been distributed or if there was an error reported during validation this will only perform the check on the local appliance. If the patch has been distributed this will perform the check on all cluster members. The same warnings may be returned from each cluster member.

- **Remove** is enabled when the patch is uploaded. Click **Remove** to remove (unstage) the patch from all cluster members.

The **Updates** pane shows the upgrade progress and when the appliance has been successfully upgraded.

Power

The Appliance Administrator or Operations Administrator can power down or restart an appliance from the web client or directly from the appliance itself.

> **CAUTION: Rebooting the appliance causes a service outage for any current users.**

You can shut down or restart your appliance from the web client. The steps follow.

To shut down an appliance

1. Navigate to **Appliance** > **Power**.
2. Under **Power**, type a **Reason** for shutting down the SPP Appliance then click **Shut Down**.
3. To confirm your action, enter the words **Shut Down** in the box and click **OK**.
4. The One Identity Safeguard for Privileged Passwords Appliance LCD screen displays `LCD service terminating`.

To start up an appliance

1. Navigate to **Appliance** > **Appliance Information**
2. Scroll to the bottom of the dialog. Under **Power**, type a **Reason** for restarting the SPP Appliance then click **Restart**. The appliance goes into maintenance mode. The user is informed when the restart is complete.
3. To confirm your action, enter the word **Restart** in the box and click **OK**.
4. The One Identity Safeguard for Privileged Passwords Appliance LCD screens display the run level status of the appliance as it is starting up. For more information, see LCD status messages on page 642.

Appliance

You can shut down or restart your appliance from the appliance itself.

Appliance: Shut down from the appliance

You can use the **Red X** button on the front panel of the appliance to shut it down. Press and hold the **Red X** button for four seconds until it displays `POWER OFF`.

CAUTION: Once the Safeguard appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.

Appliance: Restart from the appliance

After the appliance powers off, you will need physical access to start it. Press the **Green check mark** button on the front panel of the appliance for NO MORE than one second to power on the appliance.

CAUTION: Once the Safeguard appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.

Support bundle

To analyze and diagnose issues, One Identity Support may ask the Appliance Administrator or Operations Administrator to send a support bundle containing system and configuration information.

As an alternative, you can use the Recovery Kiosk to generate and send a support bundle to a Windows share. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.

Virtual appliance support bundles are generate from the web management console. For more information, see Support Kiosk on page 56..

IMPORTANT: User must remain on the page until the bundle is complete. If user refreshes or navigates away from the page the back-end bundle process continues to run to completion, but the pending web request is canceled and the bundle will not be retrievable.

To create a support bundle

1. Navigate to:
   - web client: Navigate to **Appliance** > **Support Bundle**.
2. Select **Include Event Logs** if you want to include operating system events. Unless requested by support, it is recommended to leave this unchecked because it takes much longer to generate the support bundle.
3. Select **Limit included log files** then identify the number of **Days** for which data should be collected.
4. Click **Generate Support Bundle**.
5. Browse to select a location to save the support bundle .zip file and click **Save**.
6. Send the support bundle to One Identity Support. For more information, see About us on page 690.

Time

It is the responsibility of the Appliance Administrator to manage the appliance time.

Time displays the current appliance time and allows you to enable Network Time Protocol (NTP) and set the primary and secondary NTP servers. In addition, when enabled, the NTP client status can be displayed. As a best practice, set an NTP server to eliminate possible time-related issues.

While not recommended, you can also set the appliance time on a primary (not cluster) manually.

> **CAUTION: Changing appliance time can result in unintended consequences with processes running on the appliance. For example, there could be a disruption of password check and change profiles and audit log time stamps could be misleading. Do not set the system time before or after the validity period of the Safeguard internal certificates because the appliance will not function.**

Clustered environments

NTP setting changes are made on the primary appliance in a cluster. When a replica appliance is enrolled into the cluster, it points to the primary appliance's VPN IP address as the Primary NTP Server and the NTP client service is enabled on the replica appliance. When performing a failover operation to promote a replica to be the new primary, the Primary NTP Server is preserved and applied from the 'old' primary appliance.

Warnings

The following warnings display if your local time is not within five minutes of the appliance time. One Identity recommends that you set an NTP server to eliminate possible time-related issues.

- Upon log on: `Warning: The time associated with Safeguard and your local time are off by 5 or more minutes. Contact the Safeguard administrator to correct this issue before further use.`
- On the **Settings** > **Appliance** > **Time** page: `The appliance time and your local time have a difference of 5 or more minutes. It is recommended to set an NTP server.`

To enable Network Time Protocol (NTP) and set the primary and secondary NTP servers

1. Go to **Time**:
   - web client: Navigate to **Appliance** > **Time**.
2. Select the **Enable Network Time Protocol (NTP)** check box then provide the following information:
   - **Primary NTP Server**: Enter the IP address or DNS name of the primary NTP server.

- **Secondary NTP Server**: (Optional) Enter the IP address or DNS name of the secondary NTP server.

3. Click **Save** to save your selections.

   When NTP is enabled, click **Show Details** to view the following information about the NTP client status.

   - Last Sync Time
   - Leap Indicator
   - Poll Interval
   - Precision
   - Reference ID
   - Root Delay
   - Root Dispersion
   - Source
   - Stratum
   - Last Sync Error
   - Time Since Last Good Sync

If NTP is set and you need to change the time, go to the API and use `Set-SafeguardTime`. For information about using the API, see Using the API.

To manually set the appliance time on a primary (not cluster)

To manually set the time on the appliance (primary not cluster), follow the steps below.

CAUTION: Manually setting the time should be done with caution. Time changes can cause critical data loss.

1. Go to Time:
   - web client: Navigate to **Appliance** > **Time**.
2. Clear the **Enable Network Time Protocol (NTP)** check box.
3. Click **OK**.
4. Click **Edit**.
5. For the most accurate time, complete the following steps quickly.
   a. On the **Set System Time** dialog, click **Use Client Time** to use the local time or select the date and time.
   b. Click **OK**. The **Set System Time** warning dialog displays indicating that: `Extreme time changes in Safeguard may cause critical data loss.`
   c. Type **Set Time** in the dialog box to confirm then click **OK**.

Time Zone

SPP sets a default time zone based on the location of the person performing the set up. The time zone is expressed as UTC + or – hours:minutes and is used for timed access (for example, access from 9 a.m. to 5 p.m.). It is recommended that the Bootstrap Administrator set the desired time zone on set-up. An Authorizer Administrator can also change the time zone.

To configure the time zone

1. Navigate to **User Management** > **Settings** > **Time Zone**.
2. The User Administrator can search for and select the desired time zone.
3. The User Administrator can change **Allow users to modify their own time zone**.
    - Enable the setting to let users change their time zone (the default).
    - Disable the setting to prohibit a user from changing their time zone, possibly to ensure the user conforms with policy.

Backup and Retention

Use the Backup and Retention settings to manage your SPP backups and archive servers.

It is the responsibility of the Appliance Administrator to configure the SPP backup and retention settings.

Go to Backup and Retention:

- web client: Navigate to **Backup and Retention**.

Table 20: Backup and Retention settings

Setting	Description
Archive servers	Where you add and manage archive servers for storing backup files and session recordings.
Audit Log Maintenance	Where you define the audit logs to be archived and purged as well as a schedule for performing the audit log archival task.
Backup and Restore	Where you initiate or schedule a backup, upload or download a backup file, or specify the archive server where a backup file is to be stored.
Backup Retention	Where you enable (or disable) backup retention and set the maximum number of backup files you want SPP to store on the appliance.
Authorize VM	Where you authorize the download of SPP hardware appliance

Setting	Description
Compatible Backups	backups which can then be uploaded and restored to a SPP virtual machine.

About backups

One Identity Safeguard for Privileged Passwords backs up the following:

- All settings, except:
  - Appliance IP address
  - Network Time Protocol (NTP) configurations
  - Domain Name System (DNS) configuration
- Audit logs
- All information about SPP objects:
  - Accounts
  - Account groups
  - Assets
  - Asset groups
  - Entitlements
  - Partitions
  - Users
  - User groups

SPP encrypts and signs the data before it makes it available for downloading to an off-appliance storage. Only a genuine SPP Appliance can decrypt the backup after it is uploaded to the appliance. Backups downloaded from virtual appliances can only be uploaded and restored to a virtual appliance. Backups downloaded from hardware appliances can only be uploaded and restored to a hardware appliance. A hardware backup can be downloaded as virtual compatible once the hardware appliance has been authorized for VM Compatible Backups. A VM compatible backup can be uploaded and restored to a virtual appliance.

Archive servers

Archive servers are external physical servers where you store backup files and session recordings. Use the **Archive Servers** page on the **Backup and Retention** settings view to configure and manage archive servers.

You can configure an automatic backup schedule and specify which archive server will be used to automatically archive during a scheduled backup or when manually running a backup. For more information, see Backup settings on page 168.

For more information, see Archive backup on page 167.

To view and manage archive servers

1. Navigate to Archive Servers settings:
   - web client: Navigate to **Backup and Retention** > **Archive Servers**.
2. The **Archive Servers** page displays the following information about previously configured archive servers.
   - **Name**: The name of the archive server.
   - **Archive Method**: The transfer protocol type being used.
   - **Network Address**: The network DNS name or IP address used to connect to the server over the network.
   - **Storage Path**: The file path where you want to store backup files on the archive server.
   - **Authentication Type**: The type of authentication used to access the archive server, such as Password, Directory Account, or SSH Key.
   - **SSH Host Key Fingerprint**: The fingerprint of the SSH key that Safeguard for Privileged Passwords uses to authenticate to the asset.
   - **Description**: Information about the archive server.
3. Use these tool bars buttons to perform operations.
   - **Add**: Add an archive server. For more information, see Adding an archive server on page 153.
   - **Remove**: Delete the selected archive server configuration.
   - **Edit**: Modify the selected archive server configuration.
   - **Refresh**: Update the list of archive server configurations.

Adding an archive server

Use the Archive Servers page on the Backup and Retention settings view to configure archive servers, which can then be selected to archive a backup file or assigned to an appliance to store its session recordings.

To configure an archive server

1. Go to archive servers settings:
   - web client: Navigate to **Backup and Retention** > **Archive Servers**.
2. Click **Add** and provide the following.
3. Enter the display **Name** for the archive server. Limit: 100 characters.
4. Enter **Description** information about the archive server. Limit: 255 characters.
5. For **Archive Method**, select a transfer protocol type:
   - **CIFS**: Common Internet File System
   - **SCP**: Secure Copy Protocol
   - **SFTP**: Secure File Transfer Program
6. For **Network Address**, enter a network DNS name or the IP address used to connect to the server over the network. Limit: 255 characters.
7. If you select SCP or SFTP, enter the **Port** used by SSH to log in to the managed system. Not applicable for CIFS archive mode.
8. For **Storage Path**, enter the file path where you want to store backup files on the archive server. Limit: 255 characters.
9. For **Authentication Type**, select the type of authentication to be used to access the archive server:
   - **Password** (default)
   - **Directory Account**
   - **SSH Key** (Available if an **Archive Method** of **SCP** or **SFTP** is selected.)
10. If **Directory** is the **Authentication Type**:
    a. **Account Name**: Click **Browse** to select the service account to be used to access the archive server.
    b. If you selected the **Archive Method** of **SCP** or **SFTP**, you can select **Auto Accept SSH Host Key** to have SPP automatically accept the SSH host key when it creates the archive server.
11. If **Password** is the **Authentication Type**:
    a. For **Account Name**, you can do one of the following:
       - As an Appliance Administrator, if you also have Asset Administrator permission or are a Delegated Partition Owner, you can click **Browse** to select the service account to be used to access the archive server. If a **Network Address** was entered, you will see the managed accounts for the **Network Address** or no associated **Network Address**.
         Once you select an account, a **Reset** button is available to clear the managed account selection and **Network Address** is set to the selected account's network address.
       - Enter the **Account Name** instead of browsing for a managed account.

b. **Password**: Enter the service account password.

c. If you selected the **Archive Method** of **SCP** or **SFTP**, you can select **Auto Accept SSH Host Key** to have SPP automatically accept the SSH host key when it creates the archive server.

12. If you selected the **Archive Method** of **SCP** or **SFTP** and selected **SSH Key** as the **Authentication Type**, proceed with these steps.

    a. For **Account Name**, you can do one of the following:

    - As an Appliance Administrator, if you also have Asset Administrator permission or are a Delegated Partition Owner, you can click **Browse** to select the service account to be used to access the archive server. If a **Network Address** was entered, you will see the managed accounts for the **Network Address** or no associated **Network Address**.
      Once you select an account, a **Reset** button is available to clear the managed account selection and **Network Address** is set to the selected account's network address.
    - Enter the **Account Name** instead of browsing for a managed account.

    b. In **SSH Key Generation and Deployment Settings**, select one of the following settings:

    - **Automatically generate and deploy a new SSH Key**: Enter the **Password**. Optionally, select **Auto Accept SSH Host Key** to have SPP automatically accept the SSH host key when it creates the archive server.
    - **Automatically generate a new SSH Key that I will deploy myself**: Optionally, select **Auto Accept SSH Host Key** to have SPP automatically accept the SSH host key when it creates the archive server.
    - **Import an SSH Key that I will deploy myself**: **Browse** to select the SSH Key file.

      NOTE: SPP does not currently manage the options for an authorized key. If an imported key has any options configured in the authorized keys file on the asset, these options will not be preserved when the key is rotated by SPP.

      i. Click **Browse**. On the **Import an SSH Key** dialog, click **Browse** then select the **Private Key File**.

      ii. Enter a **Password**, if desired. A password is required if the private key is encrypted.

      iii. Click **Import**.

      iv. Optionally, select **Auto Accept SSH Host Key** to have SPP automatically accept the SSH host key when it creates the archive server.

13. **Test Connection**: Click this button to verify that the appliance can communicate with this archive server. For details, see:

- About Test Connection
- Test Connection failures on archive server

14. Click **OK**.

Once you have configured your archive servers, you need to designate a target archive for both your backup files and session recordings. For backup files, see Archive backup on page 167

Audit Log Maintenance

Appliance Administrators can configure SPP to perform weekly maintenance, audit log purge, and audit log archiving to a designated archive server. Archiving audit logs allows you to keep critical and relevant data online and current while eliminating or archiving audit logs that are no longer required.

The benefits of purging audit logs include smaller backups and less audit log data to stream when enrolling a new cluster member. It is recommended you store no more than six months of audit logs on your Safeguard appliance.

The default Audit Log Maintenance configuration is to synchronize data and audit logs only on Saturday at 12 a.m.

CAUTION: Audit Log Maintenance locks the cluster. The operations can take hours depending on the amount of audit log data on the appliance, the amount of data being archived/purged, and the network between the synchronizing nodes in the cluster.

If configured to delete audit logs, each appliance will enter maintenance and be unavailable for approximately 5 minutes at some point during the audit log maintenance window.

View Audit Log Maintenance settings

1. While connected to the primary appliance, go to Audit Log Maintenance:
   - web client: Navigate to **Backup and Retention** > **Audit Log Maintenance**.
2. If configured, the following displays:
   - **Archive**: The archive server, if required by the operation.
   - **Action**: The action defined in Audit Log Maintenance.
   - **Schedule**: A description of the schedule, such as `Every Saturday at 12:00 AM`.
   - **Next Scheduled Maintenance**: The next time the scheduled maintenance will run.
   - **Last Successful Archive/Purge**: The local time of the last successful archive or purge.
   - **Last Failed Archive/Purge**: The local time of the last failed archive or purge.

- **Last Audit Log Sync**: The local time of the last audit log synchronization.
- **Last Data Sync**: The local time of the last data synchronization.

Configure and schedule Audit Log Maintenance

To define and schedule Audit Log Maintenance, configure the following. For a cluster, configure the primary appliance. Each action will take some time to process. The cluster is locked during the process and other cluster operations cannot be performed. You can check progress in the Activity Center..

1. While connected to the primary appliance, go to Audit Log Maintenance:
   - web client: Navigate to **Backup and Retention** > **Audit Log Maintenance**.
2. Click **Settings** to configure Audit Log Maintenance .
3. On the **Audit Log Maintenance** dialog, select an action:
   - **Synchronize data and audit logs only** (default action): Data and audit logs are synchronized. If any data fails to synchronize, synchronize will run again on the next day at the configured **Start time**. Audit logs are not archived or purged from the appliance.
   - **Synchronize after archiving and deleting audit logs older than __ days**. Audit logs older than the number of days specified will be archived to the specified archive server by the primary. Next, those audit logs will be removed from each node, requiring a short maintenance on each. Purged audit logs cannot be recovered. The default is 365 days. The minimum is 30 days and there is no maximum. The benefits of purging audit logs include smaller backups and less audit log data to stream when enrolling a new cluster member. It is recommended you store no more than six months of audit logs on your Safeguard appliance. This option is only available if you have configured an archive server. For more information, see Adding an archive server on page 153.
     a. Enter the **days**. Audit logs older than the number of days specified will be archived and then purged from the appliance(s). The default is 365 days. The minimum is 30 days and there is no maximum. Cluster enrollment could take longer if higher retention values are used. Data is also synchronized.
     b. Select a configured archive server in **Send to archive server**. Audit logs are archived to the specified archive server during a scheduled audit log maintenance or when **Run Now** is selected.
   - **Synchronize after deleting audit logs older than __ days**. Audit logs older than the number of **days** specified will be purged from the appliance(s). Purged audit logs cannot be recovered. The default is 365 days. The minimum is 30 days and there is no maximum. The benefits of purging audit logs include smaller backups and less audit log data to stream when enrolling a new cluster member. It is recommended you store no more than six months of audit logs on your Safeguard appliance.

4. Set the schedule for Audit Log Maintenance to run:
    a. Select the **Day of the week**. The default is Saturday.
    b. Click **Time** select the **Start Hour**. The default is 12:00 a.m.
    c. Select the time zone. The default is Coordinated Universal Time (UTC).
5. Click **OK**.

Monitoring the progress of Audit Log Maintenance

Audit Log Maintenance automatically runs the configuration settings and schedule you enter. You can also manually select to run Audit Log Maintenance. Check the results in the Activity Center based on the action. If you need to cancel the operation at any point, follow the steps in Cancel Audit Log Maintenance from the Audit Log Maintenance page

- **Synchronize data and audit logs only** (and not perform archive and delete):
    - Processing and successful completion: Audit log maintenance synchronize has both a data and audit log sync component. These only do work in a cluster. At the beginning of the operation, the cluster is locked for "ensuring data consistency". This can be viewed on both the **Audit Log Maintenance** summary and in the **Settings** > **Cluster Management**.
      The start of data synchronization is recorded with a `SynchronizingDataStarted` event. Upon completion, the `SynchronizingDataCompleted` event reports if all data was successfully synchronized or if only a portion completed. Next, the start of the audit log synchronization is recorded with the `SynchronizingAuditLogStartedEvent`. Upon completion, the `SynchronizingAuditLogCompletedEvent` will report if all audit logs were successfully synchronized or if only a portion complete.
      In order to ensure every appliance has consistent data and audit logs, synchronize must successfully synchronize all data every week.
    - Failed portions: If the complete events indicate not all sync was successful, the sync will trigger the following day at the configured start hour and retry failed portions.
- **Synchronize after archiving and deleting audit logs older than __ days:**
    - Processing: Audit log archiving selects all the audit logs after the purge date to archive. At the beginning of the operation, the cluster is locked for `Archiving and/or purging audit logs`. Audit log maintenance will proceed with the purge only if the archive is successful. On each appliance, the purge operation will determine if there is data to purge. If so, the replicas will enter maintenance one at a time to purge the data. Each appliance should be in maintenance for less than five minutes. Once complete, the primary will purge while in maintenance. The cluster lock will be released. Audit log maintenance will now proceed to the synchronize operations as detailed in the bullet above.
    - Successful: When the archive is successfully sent to the archive server, it will generate an `ArchiveTaskSucceeded` event. If purge is required and successful, it will generate the `AuditLogPurged` event. The cluster lock will be released and the `SchedulerJobSucceeded` event will mark the end of the archive/purge

operations. Audit log maintenance will continue on to synchronize as detailed above.

- Failed: If the primary appliance is unable to archive the audit logs, there will be no `ArchiveTaskSucceeded` event and there will be no subsequent purge. The data will remain on all appliances. The archive/purge operation will complete with a `SchedulerJobFailed` event containing `Job ID = core.AuditLogMaintenance`. You can see the reason for the failure in the event. Audit log maintenance will continue on to synchronize as detailed above.

- **Synchronize after deleting audit logs older than __ days**:
  - Processing: Audit log purging enumerates all the audit logs after the purge date to delete from each appliance in the cluster. The data cannot be recovered. At the beginning of the operation, the cluster is locked for `Archiving and/or purging audit logs`. On each appliance, the purge operation will determine if there is data to purge. If so, the replicas will enter maintenance one at a time to purge the data. Each appliance should be in maintenance for less than five minutes. Once complete, the primary will purge while in maintenance. The cluster lock will be released. Audit log maintenance will now proceed to the synchronize operations as detailed in the bullet above.
  - Success: If purge is required and successful, it will generate the `AuditLogPurged` event. The cluster lock will be released and the `SchedulerJobSucceeded` event will mark the end of the archive/purge operations. Audit log maintenance will continue on to synchronize as detailed above.
  - Failed: If the primary appliance is unable to delete the audit logs, the operation will complete with a `SchedulerJobFailed` event containing `Job ID = core.AuditLogMaintenance`. You can see the reason for the failure in the event. Audit log maintenance will continue on to synchronize as detailed above.

Manually run Audit Log Maintenance

You can manually run Audit Log Maintenance. The same operations detailed above based on the Audit Log Maintenance configuration execute. Each action will take some time to process. The cluster is locked during the process and other cluster operations cannot be performed. You can check progress in the Activity Center..

1. While connected to the primary appliance, go to Audit Log Maintenance:
   - web client: Navigate to **Backup and Retention** > **Audit Log Maintenance**.
2. Click **Settings** to ensure the Audit Log Maintenance configuration is correct.
3. Click **Run Now** to run Audit Log Maintenance as configured. You will be presented with a confirmation dialog box. How you proceed will depend on the action you selected:
   - If the action is **Synchronize data and audit logs only** (and not perform archive and delete), the **Synchronize Data and Audit Logs** dialog box displays.

    - Type in **Synchronize** in the text box then click **OK**. To monitor progress in the Activity Center, see Monitoring the progress of Audit Log Maintenance.
  - If the action is **Synchronize after archiving and deleting audit logs older than __ days**, the **Archive** dialog box displays with the name of the archive server.
    - Type **Archive** in the text box and click **OK**. To monitor progress in the Activity Center, see Monitoring the progress of Audit Log Maintenance.
  - If the action is **Synchronize after deleting audit logs older than __ days**, the **Purge Audit Log** dialog displays indicating that the audit log will be purged according to the retention policy (the number of days you entered). Purged audit logs cannot be recovered.
    - Type **Purge** in the text box and click **OK**. To monitor progress in the Activity Center, see Monitoring the progress of Audit Log Maintenance.

Cancel Audit Log Maintenance from the Audit Log Maintenance page

When Audit Log Maintenance is running, the cluster is locked and a **Cancel** button is available. When you click **Cancel**, you will be presented with an **Unlock Cluster** confirmation dialog. Enter **Unlock Cluster** and click **OK**. The cluster lock is released immediately, however you must monitor Activity Center as follows to ensure the operations are complete. For more information, see Monitoring the progress of Audit Log Maintenance on page 158.

- **Synchronize data and audit logs only**: When you cancel, the lock is release immediately, however you must monitor Activity Center for completion of the work. In the Activity Center, wait for the `SynchronizingDataCompletedEvent` then the `SynchronizingAuditLogsCompletedEvent` to appear before proceeding with other clustering operations to ensure all nodes in the cluster hold all of the audit data. Once canceled, the cluster will try and complete the audit log synchronization on the Audit Log Management **Start Hour** on the next day.
- **Synchronize after archiving and deleting audit logs older than __ days**: When you cancel, the lock is release immediately, however you must monitor Activity Center for completion of the work. If you elect to cancel while the cluster is locked for **Archiving and/or purging audit logs**, monitor Activity Center for the `SchedulerJobSucceeded` or `SchedulerJobFailed` event, containing `Job Id = core.AuditLogMaintenance`, indicating the archive/purge has completed. Audit Log Maintenance will continue to synchronize regardless. You will also need to cancel once you see the cluster is locked for `Ensuring data consistency`. Monitor the Activity Center for the `SynchronizingAuditLogCompleted` event indicating the operation completed. It is now safe to continue with your clustering operation.
- **Synchronize after deleting audit logs older than __ days**: When you cancel the lock is release immediately, however you must monitor Activity Center for completion of the work. If you elect to cancel while the cluster is locked for `Archiving and/or purging audit logs`, monitor Activity Center for the `SchedulerJobSucceeded` or `SchedulerJobFailed` event, containing `Job Id = core.AuditLogMaintenance`, indicating the archive/purge has completed. Audit Log Maintenance will continue to synchronize regardless. You will also need to cancel once you see the cluster is locked

for `Ensuring data consistency`. Monitor the Activity Center for the `SynchronizingAuditLogCompleted` event indicating the operation completed. It is now safe to continue with your clustering operation.

To cancel Audit Log Maintenance from Cluster Management

You can also cancel Audit Log Maintenance from Cluster Management by unlocking the cluster with the following steps. For more information, see Unlocking a locked cluster on page 597.

1. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
2. On **Cluster Management**, a banner like the following displays: `Archiving and/or purging audit logs` and the **Start Time** displays. The message reminds you that the cluster is locked during the process and other cluster operations cannot be performed. The cluster will unlock automatically when the operation is complete.
3. Click the lock icon in the upper right corner of the warning banner.
4. In the **Unlock Cluster** confirmation dialog, enter **Unlock Cluster** and click **OK**.

   This will release the cluster lock that was placed on all of the appliances in the cluster and close the operation.

IMPORTANT: Care should be taken when unlocking a locked cluster. It should only be used when you are sure that one or more appliances in the cluster are offline and will not finish the current operation. If you force the cluster unlock, you may cause instability on an appliance, requiring a factory reset and possibly the need to rebuild the cluster. If you are unsure about the operation in progress, do NOT unlock the cluster.

Backup and Restore

It is the responsibility of the Appliance Administrator to manage Safeguard for Privileged Passwords backups.

As a best practice, store backups on an archive server that is external from the appliance so that the backup image is available for restoration even if there is a catastrophic disk or hardware failure. Keep only a minimum number of backup files on the appliance. After you download or archive the Safeguard Backup Files (.sgb), use **Delete** to remove them. You can set the maximum number of backup files you want Safeguard for Privileged Passwords to retain on the appliance in Backup and Retention.

For maximum backup protection, Appliance Administrators can configure the cluster wide GPG public key or password encryption. Either will protect all subsequent backups generated from each appliance in the cluster. GPG protection will apply when downloaded or archived. Password protection will apply when generated. For details, see:

- Backup protection settings
- Upload a backup
- Restore a backup

Go to Backup and Restore:

- web client: Navigate to **Backup and Retention** > **Backup and Restore**.

The **Backup and Restore** page lists this information for the backups that are currently in the database.

Table 21: Backup and Restore: Properties

Property	Description
Date	The date of the backup
Progress	The status of the backup: Running or Complete
File Size (MB)	The size of the backup file in megabytes
Appliance Name	The name of the appliance
Appliance Version	The version of the SPP Appliance
Protection Type	Hover over an icon to view the type of protection: • (default) Standard protection: No password or GPG key is required. • GPG public key protection: A private key is required to upload the backup to be restored. • Password protection: A password is required to restore the backup.
User	The name of the user that created the backup
Last Archived Date	The date the selected backup ran
Archive Server Name	The name of the server on which the backup was archived
File Name	The Safeguard backup file name which is an .sgb file.

Use these toolbar buttons to manage SPP backups.

Table 22: Backup and Restore: Toolbar

Option	Description
Run Now	Create a backup copy of the data that is currently on the appliance. For more information, see Run Now on page 163.
Remove	Remove the selected backup file from the **Backups** page and the SPP database. The backup is immediately removed.
Download	Save the selected backup file in a location on your appliance. For more information, see Download a backup on page 164.

Option	Description
Download VM Compatible	Use this option to download a VM compatible backup, which can then be uploaded and restored on a SPP virtual machine. In order to download a VM compatible backup it must have been created with password or GPG public key protection settings. To enable the option to download a VM compatible backup of a hardware appliance, see Authorize VM Compatible Backups. IMPORTANT: You cannot upload a backup to hardware that has been downloaded from hardware as VM compatible.
Upload	Retrieve a backup file from a file location and add it to the **Backups** page list. For more information, see Upload a backup on page 165.
Restore	For the selected backup file, overwrite the current data and restore SPP to the selected backup. For more information, see Restore a backup on page 166.
Archive	Store the selected backup file on an external archive server. For more information, see Archive backup on page 167.
Settings	• **Backup Settings**: Where you configure an automatic backup schedule. For more information, see Backup settings on page 168. • **Backup Protection Settings**: Where you set backup encryption on an appliance or on a primary appliance for cluster-wide protection. For more information, see Backup protection settings on page 170.
Refresh	Update the list of backup files on the **Backups** page.

Run Now

You can click Run Now to manually trigger and create a new backup. If password or GNU Privacy Guard (GPG) encryption is set for appliance or on the primary appliance for cluster-wide encryption, those encryption settings are enforced when you select Run Now.

If you have selected **Send to archive server**, the backup will be sent to the archive server. For more information, see Backup settings on page 168.

To create a new backup

1. Navigate to Backup and Restore:
   - web client: Navigate to **Backup and Retention** > **Backup and Restore**.

2. Click **+ Run Now**. In the web client, an **Adding backup file** progress bar displays to let you know the process is **Running**.
3. If password encryption is required on an appliance or a primary appliance for cluster-wide backup encryption, you are prompted to enter the password. If encryption is set, make sure the password or private GPG key is available for restoring the backup later, if necessary. For more information see, Backup and restore, Backup protection settings.
4. Verify that the Safeguard Backup File (.sgb) has been created.

CAUTION: If you restore a backup that is older than the Maximum Password Age set in the Local Login Control settings, all user accounts (including the bootstrap administrator) will be locked out and you will have to reset all of the user account passwords. To avoid this situation, you can reset the Maximum Password Age to zero before you perform the backup, then reset it after the restore.

TIP: As a best practice, perform backups more frequently than the **Maximum Password Age** setting.

CAUTION: SPP can not restore any access request workflow events in process at the time of a backup.

CAUTION: When restoring a backup that was created with a Hardware Security Module integration in place, the encryption key used at the time of the backup creation needs to still be present and accessible by the SPP appliance. If not, the appliance will not be able to verify the Hardware Security Module configuration used to encrypt the data in the backup. You will be allowed to continue with the restore, however the SPP appliance will most likely Quarantine in the process, so this is not recommended.

Download a backup

SPP allows you to save a selected backup file in a location on your computer. SPP copies the selected backup file; it does not remove the backup from the list displayed on the Backup and Restore page. An Appliance Backup Downloaded event is generated and sent to the audit log when a backup is downloaded from the appliance. The event will note if the backup was downloaded as VM compatible. To remove a file from the list display, select the file and click **Remove**.

To download the backup file

1. Go to Backup and Restore:
   - web client: Navigate to **Backup and Retention** > **Backup and Restore**.
2. Select a backup file:

- **Download**: Use this option to save the selected backup file in a location on your appliance.
- **Download VM Compatible**: Use this option to download a VM compatible backup, which can then be uploaded and restored on a Safeguard virtual machine. In order to download a VM compatible backup it must have been created with password or GPG public key protection settings. This is only available on hardware appliances once Authorize VM Compatible Backups has been requested and approved.

  IMPORTANT: You cannot upload a backup to hardware that has been downloaded from hardware as VM compatible.

3. The .sgb file is downloaded to the browser's Download folder as defined in the browser settings. The file has a name similar to the following which includes the date: `946d66a4fecb4359a8b01fab75519d80_Safeguard_Backup_20200617-165625.sgb`

   NOTE: There is no difference in the downloaded backup filename for regular download versus VM Compatible download.

Upload a backup

SPP allows you to retrieve a Safeguard Backup File (.sgb) from a file location and add it to the **SPP Backup and Restore** page list for the appliance. For more information, see Restore a backup on page 166.

An Appliance Backup Uploaded event is generated and stored in the audit log when a backup is successfully uploaded to the appliance. An Appliance Backup Upload Failed event is generated and stored in the audit log when a backup upload fails on the appliance.

Backups generated and downloaded from a virtual machine can only be uploaded to a virtual machine. Backups generated and downloaded on hardware appliances can only be uploaded to a hardware appliance. Backups generated and downloaded as VM compatible on hardware appliances can only be uploaded to virtual machines.

To upload a backup file

IMPORTANT: Once you start uploading a backup, do not leave or refresh the page. Doing so will cause the browser to lose track of the upload and you will have to restart the process.

1. If a GPG public key was used to encrypt the backup, the private key holder must decrypt the Safeguard Backup File (.sgb) before it can be uploaded to SPP. For more information, see Backup protection settings on page 170.
2. To upload Safeguard Backup File (.sgb), go to Backup and Restore:
   - web client: Navigate to **Backup and Retention** > **Backup and Restore**.
3. Click **Upload**.

4. Browse to select the backup file and click **Open**. The **Uploading backup file** progress bar displays. When complete, the file is uploaded and is now available to be restored. For more information, see Restore a backup on page 166.

Restore a backup

SPP allows you to restore the data on your appliance with data from a selected backup. SPP does not restore the appliance IP address, NTP settings, or the DNS settings.

To verify that the settings are correct after a restore, go to:

- web client: Navigate to **Appliance** > **Appliance Information**.

There are special considerations for restoring a clustered appliance. For more information, see Using a backup to restore a clustered appliance on page 591.

CAUTION: If you restore a backup that is older than the Maximum Password Age set in the Local Login Control settings, all user accounts (including the bootstrap administrator) will be disabled and you will have to reset all of the user account passwords or SSH keys. If your bootstrap administrator's password is locked out, you can reset it from the Recovery Kiosk. For more information, see Admin password reset on page 650.

CAUTION: When restoring a backup that was created with a Hardware Security Module integration in place, the encryption key used at the time of the backup creation needs to still be present and accessible by the SPP appliance. If not, the appliance will not be able to verify the Hardware Security Module configuration used to encrypt the data in the backup. You will be allowed to continue with the restore, however the SPP appliance will most likely Quarantine in the process, so this is not recommended.

Version considerations when restoring a backup

An Appliance Administrator can restore backups as far back as SPP version 6.0.0.12276. Only the data is restored; the running version is not changed.

You cannot restore a backup from a version newer than the one running on the appliance. The restore will fail and a message like the following displays: `Restore failed because backup version [version] is newer then the one currently running [version].`

The backup version and the running version display in the Activity Center logs that are generated when Safeguard starts, completes, or fails a restore.

To restore the SPP appliance from a backup

1. Go to Backup and Restore:
   - web client: Navigate to **Backup and Retention** > **Backup and Restore**.

2. Select a backup. If the backup file is not listed, you can ↥ **Upload** the .sgb backup file. For more information, see Upload a backup on page 165.
3. Click ⟲ **Restore**.

   If a problematic condition is detected, ⚠ **Warning for Restore of Backup** displays along with details in the **Restore Warnings, Warning X of X** message. Click **Cancel** to stop the restore process and address the warning or click **Continue** to move to the next warning (if any) or complete the process.
4. If the backup is protected by a password, the **Protected Backup Password** dialog displays. Type the password in the **Enter Backup Password** text box. If the password entered is not correct, the **OK** button is disabled and you cannot proceed. For more information, see Backup protection settings on page 170.
5. When the **Restore** dialog displays, enter the word **Restore** in the box and click **OK**.

   SPP automatically restarts the appliance, if necessary.
6. After restoring from backup verify that the following are set correctly.
   - Check the archive server in the automated backup schedule. If necessary, set the correct archive server. For more information, see Archive backup on page 167.
   - Check the archive server in the session archive settings. If necessary, set the correct archive server. If you used the embedded sessions module and had an archive server configured, the archive server must be configured to play back the archived sessions.
   - If you restored a backup to a different appliance, managed networks will no longer have any assigned appliances. Password and SSH key management and discovery tasks will fail. For more information, see Managed Networks on page 201.
7. Once the appliance is fully operational, it asks you to restart the client. All modifications to Safeguard for Privileged Passwords objects since the backup was created will be lost.

> ⚠ **CAUTION: After a restore, requesters, approvers, and reviewers will not have access to any access request workflow events that were in process at the time of the backup. The Activity Center displays those workflow events as incomplete.**

Archive backup

SPP allows you to store backup files on an external archive server.

To archive a backup file

The archive server must be set up. For more information, see Adding an archive server on page 153.

1. Go to Backup and Restore:
    - web client: Navigate to **Backup and Retention** > **Backup and Restore**.
2. Select the backup to be archived.
3. Proceed to archive the backup:
    - web client: Click **Archive**. On the **Archive Servers** dialog, choose an archive server.

SPP copies the backup file to the archive server.

Backup settings

You can configure an automatic backup schedule.

If you schedule a backup and a backup has already occurred for that interval (minute, hour, day, week, or month), another backup will not execute until the following minute, hour, day, week, or month. For example, if a backup has already occurred today and you set the backup schedule to run a daily backup, SPP will not run the backup until tomorrow.

The backup schedule window end time must be after the start time.

Backup files to retain

In addition to completing the settings in the steps which follow, you can configure the maximum number of backup files you want SPP to store on the appliance on the Backup Retention page.

To configure the backup schedule

1. Go to Backup and Restore:
    - web client: Navigate to **Backup and Retention** > **Backup and Restore**.
2. Based on the client you are using, do one of the following:
    - web client: Click **Settings**.
3. In the **Backup Settings** dialog, specify the backup schedule.
4. Enter the schedule.
    - Select a time frame:
        - **Never**: The job will not run according to a set schedule. You can still manually run the job.
        - **Minutes**: The job runs per the frequency of minutes you specify. For example, `Run Every 30/Minutes` runs the job every half hour over a 24-

hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.

- **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select `Run Every 2/Hours/@ minutes after the hour 15`.
- **Days**: The job runs on the frequency of days and the time you enter.

  For example, `Run Every 2/Days/Starting @ 11:59:00 PM` runs the job every other evening just before midnight.
- **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

  For example, `Run Every 2/Weeks/Starting @ 5:00:00 AM` and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.
- **Months**: The job runs on the frequency of months at the time and on the day you specify.

  For example, If you select `Run Every 2/Months/Starting @ 1:00:00 AM` along with `Day of Week of Month/First/Saturday`, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click **+ Add** or **— Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter `Run Every 10/Minutes` and set **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

  For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

  For days, enter `Run Every 2/Days` and set **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

5. In **Send to archive server**, select an already configured archive server to store the backup files externally from the appliance during a scheduled backup or when manually running a backup.This option is only available if you have configured an archive server. For more information, see Adding an archive server on page 153.

6. You can select the **Backup Protection** settings. For more information, see Backup protection settings on page 170.
7. Click **OK** to save your changes and leave the page. In the web client, you can click **Apply** to save your changes and stay on the page.

Backup protection settings

For maximum protection, set backup encryption on an appliance or on a primary appliance for cluster-wide protection. You may encrypt a Safeguard Backup File (.sgb) with one of the following methods:

- Standard (default): No password or GPG key is required.
- Password: You can enter any password value. You must have the password to restore the backup.

  CAUTION: Make sure to save the password in a safe vault. There is no way to recover the password needed to restore the backup.

- GNU Privacy Guard (GPG) public key (RSA only): You can upload a .txt file with the public key and meta data or copy and paste the public key and meta data to SPP. A backup file created with a GPG public key is encrypted when it is downloaded or archived. Only the private key holder can decrypt the backup file prior to the file being uploaded and restored. Once the private key holder decrypts the backup, the backup is the same as a backup generated when only appliance protection was selected.

  CAUTION: Make sure to save the GPG private key in a safe vault. There is no way to unencrypt the GPG protected file without the private key.

Once set, future backups created manually or automatically are protected.

SPP detects all attempted uploads of an invalid backup. If a backup is GNU Privacy Guard (GPG) encrypted, a message like the following displays: `The uploaded file could not be validated as a genuine Safeguard backup image. It has been blocked from the appliance.` An audit event is created for the failed backup load with the error reasons which include an invalid signature.

For details, see:

- Upload a backup
- Restore a backup

To configure backup protection

1. If you will use GPG key protection, generate your public key file and create a .txt file to be uploaded or copy and pasted.

2. Go to Backup and Restore:
   - web client: Navigate to **Backup and Retention** > **Backup and Restore**. Then, click **Settings**.
3. From the **Backup Settings** dialog, select the type of backup protection for the appliance. The settings on a primary appliance are replicated to the cluster. The settings are read-only on each cluster node.
   - **Appliance Protection Only**: This is the default and includes no password or GPG Key protection of the backup. The backup is only encrypted as a Safeguard genuine backup.
   - **Add Password Protection**: Once selected, enter the password in the **Backup Password** text box. If a password already exists, a static number of dots display. You can type in a new password in place of the existing password and then confirm the password. The password you type in is used for backups made from the time the password is set until it is changed. Make sure to keep the password information in a safe vault.
   - **Add GPG Key Protection**: Once selected, do one of the following:
     - Click **Browse** to upload the public key file from a .txt file you created earlier.
     - Paste the public key information generated earlier into the text box.

     When you navigate back to this dialog, you will see the name, fingerprint, and the detail to identify the public key file.

     The GPG public key you submit is used for backups generated from the time protection is set until it is changed. Once a backup is generated while GPG is set, it will always be downloaded or archived with the GPG public key encryption, regardless of any settings changed on the appliance after it is generated. The GPG public key encryption stays with the backup metadata. In addition, if you upload the backup to another appliance, downloading the backup again will encrypt it with the same GPG public key originally provided.
4. Click **OK**.

Backup Retention

It is the responsibility of the Appliance Administrator to configure the maximum number of backup files you want SPP to store on the appliance.

To configure the appliance backup retention settings

1. Go to Backup Retention:
   - web client: Navigate to **Backup and Retention** > **Backup Retention**.

2. Enter the maximum number of backup files you want to store on the appliance. You can enter 0 to 40 for the number of backup files that will be stored on the appliance. Then click **Save**.

Once SPP saves the maximum number of backup files, next time it performs a backup, it deletes the backup file with the oldest date.

Authorize VM Compatible Backups

The SPP web client allows you to generate a backup on a hardware appliance which can then be uploaded and restored on a Safeguard virtual machine.

IMPORTANT: Due to the potential security risk with migrating from a hardware appliance to a virtual machine, the Appliance Administrator making the request is required to contact One Identity Support as part of this process before they will be able to complete enabling this feature. This approval is indicated by the **Not Authorized**/**Authorized** indicator at the top of the **Authorize VM Compatible Backups** page.

IMPORTANT: You cannot upload a backup to a hardware appliance which was previously downloaded from hardware as VM compatible. Such a backup can only be uploaded to a Safeguard virtual machine.

IMPORTANT: This feature is not available on a replica within a cluster.

To authorize generating a hardware appliance backup for use on a virtual machine

1. Navigate to **Backup and Retention** > **Authorize VM Compatible Backups**.
2. In the **Challenge Request User Identifier** field, enter the name of the user requesting permission for the backup to be generated.
3. Click **Generate Request**.

   NOTE: Only one challenge request can be active at a time. If there is a pending challenge request already active, you can cancel the active request by selecting the **Invalidate Existing Challenge Request** check box before generating a new request.
4. A **Challenge Request** text box will appear. This text box contains the information needed by One Identity to confirm the VM compatible backup authorization request is valid. Use one of the following options to copy the information:
   - **Copy Request**: This copies the challenge request to your clipboard.
   - **Download Request**: This downloads the challenge request to a text file.
5. Contact One Identity Support regarding your request to authorize the download of VM compatible backups from a hardware appliance. When requested, send the copied or downloaded challenge request to One Identity Support.
6. Once One Identity Support has confirmed the request, a challenge response will be sent back. This text needs to be copy/pasted or uploaded (using the **Browse** button)

to the **Challenge Response** text box.

7. Click **Verify Response** to confirm the request as been approved.

   Once confirmed, an **Authorized** indicator will be displayed at the top of the **Authorize VM Compatible Backups** page. The **Download VM Compatible** option will now be available through the button on the Backup and Restore page on hardware appliances. In order to download a VM compatible backup it must have been created with password or GPG public key protection settings.

   You can use the **Remove Authorization** button to disable this feature. To reenable a new Challenge Request must be sent to One Identity Support.

Certificates

Use the Certificate settings to manage the certificates used to secure One Identity Safeguard for Privileged Passwords. The panes on this page display default certificates that can be replaced or user-supplied certificates that have been added to SPP.

It is the responsibility of the Appliance Administrator to manage the Certificate Signing Requests (CSRs) used by SPP.

Go to Certificates:

- web client: Navigate to **Certificates**.

Table 23: Certificates settings

Setting	Description
Audit Log Signing Certificate	Where you manage the audit log signing certificate used to validate audit logs stored on an archive server. When the audit log is exported, the log is signed with this certificate to ensure that it is legitimate and has not been tampered with after export.
Certificate Signing Request	Where you can view and manage certificate signing requests (CSRs) that have been issued by SPP. CSRs that may be created in SPP include: Audit Log Signing Certificate, SMTP Client Certificate, SSL Certificates, or Syslog Client Certificates.
Hardware Security Module Certificates	Where you manage client and server Hardware Security Module certificates. These certificates are used for connecting to Hardware Security Module devices.
SMTP Certificate	Where you manage SMTP client certificates.
SSL/TLS Certificates	Where you manage SSL/TLS certificates, including installing certificates or creating CSRs to enroll a public SSL/TLS certificate. This certificate is used to secure all HTTP traffic.
Syslog Client Certi-	Where you manage the syslog client certificate used to secure

Setting	Description
ficate	traffic between SPP and the syslog server.
Trusted CA Certificates	Where you add and manage certificates trusted by SPPand used to verify the chain of trust on certificates for various usages. For example , a trusted certificate may be your company's root Certificate Authority (CA) certificate or an intermediate certificate .

About Certificate Signing Requests (CSRs)

You can create a certificate signing request (CSR) in SPP. The private key is kept securely on the SPP Appliance and is not released. The public key and details are in an encoded text file. Here is the process:

1. Create a CSR through SPP. See:
    - Creating an audit log Certificate Signing Request
    - Creating an SMTP Certificate Signing Request
    - Creating an SSL/TLS Certificate Signing Request
    - Creating a syslog client Certificate Signing Request
2. Submit the encoded text file to a Certificate Authority (CA) to create an appropriate X509 certificate that is trusted by other entities trusting the CA.
3. Install the certificate generated by the CA on SPP where it is associated with the private key. See:
    - Installing an audit log certificate
    - Installing an SMTP certificate
    - Installing an SSL/TLS certificate
    - Installing a syslog client certificate
4. If necessary, add the CA certification to Trusted Certificates in SPP. For more information, see Trusted CA Certificates on page 193..

The certificate infrastructure in One Identity Safeguard for Privileged Passwords consists of the following.

Replaceable certificates

One Identity Safeguard for Privileged Passwords ships with the following default certificates which are untrusted and are meant to be replaced:

- Audit Log Signing Certificate
- SMTP Certificate

- SSL/TLS Certificates
- Syslog Client Certificate

User-supplied certificates

You can specify the security certificates to be used. When replacing or adding certificates, keep the following considerations in mind:

- SPP supports Certificate Signing Requests (CSRs) to enroll any type of certificate. CSRs use the Public-Key Cryptography Standard (PKCS) #10 format.
- For imports, SPP must access the relevant network resources to validate the CRL end points specified in the signed CSR.
- For uploading certificates with private keys, SPP supports .pfx (or .p12) files that follow the PKCS #12 standard.
- For installing certificates generated with a CSR, SPP supports DER Encoded Files (.cer, .crt, or .der) and PEM Encoded Files (.pem).
- For SSL/TLS certificates, SPP allows you to upload or use a CSR to enroll multiple certificates that can then be applied to different appliances.
- SPP provides an SSL/TLS certificate store that allows you to assign any uploaded or enrolled a certificate to any appliance.
- Consider if the server's signing authority certificate must be added to the Trusted Certificates store in SPP. For example, prior to adding an asset that uses SSL/TLS server certificate validation, you must add the signing authority certificate to the Trusted Certificates store. Or, if you uploaded a syslog certificate with a private key, you may upload the certificate's root CA to the list of trusted certificates. For more information, see Trusted CA Certificates on page 193..

Audit Log Signing Certificate

The **Audit Log Signing Certificate** pane on the Certificates setting page displays details about the certificate used to sign the audit log files saved to an archive server.

The audit log signing certificate proves that the audit logs were created by and came from a particular SPP (SPP) cluster.

Define an audit log signing certificate

You can have only one audit log signing certificate defined, which is used by all SPP Appliances in the same cluster. A default audit log signing certificate is supplied, however it is recommends that you load your own. If you do not upload a certificate, the default is used. For more information, see Installing an audit log certificate on page 178.

Generate a Certificate Signing Request (CSR)

Once the audit log signing certificate is defined, it is recommended you generate the Certificate Signing Request (CSR) using **Create Certificate Signing Request (CSR)** . For more information, see Creating an audit log Certificate Signing Request on page 177.

A common signature format is used. Each audit log archive is hashed using the SHA256 hash algorithm. The hash value is signed with the audit log signing certificate private key using RSA signing with PSS signature padding. The signature file is created using the same file name as the archive file but with the .sig file extension.

How to use the signing certificate

This signing certificate is used by administrators who want to verify that the exported audit log history originated from their SPP cluster.

The certificate's public key must be available to validate the signed audit log and, in the case of a certificate chain, the certificate's issuer.

> IMPORTANT: Starting with the 6.6 version of the `Safeguard-ps` PowerShell cmdlets, a new cmdlet called `Test-SafeguardAuditLogArchive` has been added. This cmdlet will verify all of the audit log files in the archived zip file in one command and show the results for each file. When running the cmdlet you are validating the signature of each individual log file within the zip file; you are not validating the signature of the zip file. See OneIdentity/safeguard-ps.
>
> The following instructions are also provided should you wish to use OpenSSL or would like more information on what the PowerShell cmdlet does.

1. Get the audit log public certificate. See the following:
   - If you are using your own PKI, the public certificate should be available
   - Get the public certificate in Base64 format from the SPP API at: `GET /AuditLog/Retention/SigningCertificate`
2. If the public certificate is obtained from the API, save the Base64 data to `cert.pem`
3. Use OpenSSL to convert the pem file to a public key file.
   - `openssl x509 -pubkey -in cert.pem -noout > cert.pub`
4. Use OpenSSL to verify that the audit log file has been signed and the contents are valid.
   - `openssl dgst -sha256 -sigopt rsa_padding_mode:pss -sigopt rsa_pss_saltlen:-1 -signature <signature-file>.sig -verify cert.pub <audit-log-file>`

Manage audit log signing certificates

Go to Audit Log Signing Certificate:

- web client: Navigate to **Certificates** > **Audit Log Signing Certificate**.

The following properties and controls are available to manage your audit log signing certificate.

Table 24: Audit Log Certificates: Properties

Properties/Controls	Description
Refresh	Click **Refresh** to update the certificate displayed on the **Audit Log Certificates** pane.
Subject	The name of the subject (such as user, program, computer, service or other entity) assigned to the certificate when it was requested.
Thumbprint	A unique hash value that identifies the certificate.
Use Default	Click **Use Default** to reset the certificate back to the default supplied by SPP.
Add Certificate	Click **Add Certificate** and select one of the following options to replace the default certificate with a new certificate: • **Install Certificate generated from CSR** • **Install Certificate with Private Key** • **Create Certificate Signing Request (CSR)**

Creating an audit log Certificate Signing Request

If you do not want to use a default sessions certificate provided with SPP, you can enroll a certificate using a Certificate Signing Request (CSR) to replace the default certificate. You can return to the default certificate later.

To create a CSR for an audit log signing certificate

1. Go to Audit Log Signing Certificate:
   - web client: Navigate to **Certificates** > **Audit Log Signing Certificate**.
2. Click **Add Certificate** and select **Create Certificate Signing Request (CSR)**.
3. In the **Audit Log Signing Certificate** dialog, enter the following information:
   a. **Subject (Distinguished Name)**: Enter the distinguished name of the person or entity to whom the certificate is being issued in the proper format like: cn=common name,ou=organizational unit,o=organization. Using the format example, `cn=sam doe,ou=marketing,o=mycompany`. Maximum length is 500 characters.
      - Click **Use Distinguished Name Creator** to create the distinguished name based on your entries in **Fully Qualified Domain Name** (required), **Department**, **Organization**, **City/Locality**, **State/County/Region**, and **Country**.

b. **Subject Alternate Names (DNS)**: Optionally, enter the Data Source Name (DNS) name of the server that will be protected by this certificate. For example, this might be the DNS names of all of the appliances in the SPP cluster.

   If the DNS name changes, you must generate a new certificate.

c. **Subject Alternate Names (IP Address)**: Optionally, enter the IP addresses of the server that will be protected by this certificate. For example, this might be the IP addresses of all the appliances in the SPP cluster.

   If the IP address changes, you must generate a new certificate.

d. **Key Size**: Select the bit length of the private key pair. The bit length determines the security level of the SSL certificate. A larger key size is more secure but encryption is slower.

   - 1024
   - 2048 (default)
   - 4096

4. Click **OK** . You are prompted with a message like: `Please save and submit the following Certificate Signing Request to a Certificate Authority (CA).`
5. Click **Save** to save the CSR to a file. If you do not save the CSR, you will have to generate another one.
6. In the **Certificate Signing Request** pane, click **Refresh** to update the list of certificates added.

Installing an audit log certificate

It is recommended that you not use the default certificate provided with SPP. Instead, replace it with another certificate with a private key.

To replace the default certificate with your own, the certificate must have the following:

- Key Usage extension with the Digital Signature bit set.
- Key Usage extension with the Non-Repudiation bit set.

CSRs may be installed in the following formats.

- Install Certificate generated from CSR including:
  - DER Encoded Files (.cer, .crt, or .der)
  - PEM Encoded Files (.pem)
- Install Certificate with Private Key including:
  - PKCS#12 (.p12 or .pfx)
  - Personal Information Exchange Files (.pfx)

To install an audit log signing certificate

1. Go to Audit Log Signing Certificate:
   - web client: Navigate to **Certificates** > **Audit Log Signing Certificate**.
2. Click **Add Certificate** for the sessions certificate to be replaced. Select the appropriate option:
   - **Install Certificate generated from CSR**
   - **Install Certificate with Private Key**
3. **Browse** and select the certificate file then click **Open**.
4. If you are installing a certificate with a private key, a dialog box displays. Enter the case sensitive passphrase to import the certificate. If the certificate does not have a private key passphrase, leave the field empty and click **OK**.
5. Once installed, this new certificate will replace the default certificate listed on the **Audit Log Signing Certificate** pane.

If an audit log signing certificate upload fails, the audit log reflects: `AuditLogSigningCertificateUploadFailed`.

To use the default certificate

You can use the default sessions certificate provided with SPP

1. Go to Audit Log Signing Certificate:
   - web client: Navigate to **Certificates** > **Audit Log Signing Certificate**
2. Click the **Use Default** button for the audit log signing certificate to be replaced with the default.
3. On the warning **Use Default** dialog, type in the word `Default` to confirm you will be returning to the default certificate.
4. Click **Default** to confirm.

Certificate Signing Request

Some certificates require a digital signature before a certification authority (CA) can process the certificate request. You may need to create a certificate signing request in SPP for the following:

- Audit Log Signing Certificate
- SMTP Certificate
- SSL/TLS Certificates
- Syslog Client Certificate

The Certificate Signing Request pane displays details about any certificates enrolled via Certificate Signing Requests (CSRs). From this pane, you can also delete a CSR.

Go to Audit Log Signing Certificate:

- web client: Navigate to **Certificates** > **Certificate Signing Request**.

Certificates enrolled via a CSR appear on this pane including the following details.

Table 25: Certificate Signing Request: Properties

Property	Description
Subject	The distinguished name of the person or entity to whom the certificate is being issued
Certificate Type	The type of certificate requested: • Audit Log Signing Certificate • SSL Certificate
Key Size	The bit length of the private key pair
Thumbprint	A unique hash value that identifies the certificate
Expiration Date (web client)	The date the CSR expires, if any.
Alternate DNS Names	Additional or alternate host names (such as, sites or common names) that were specified when the certificate was requested.. For more information, see Creating an audit log Certificate Signing Request on page 177.
Alternate IP Addresses	Additional or alternate host names (such as, IP addresses or common names) that were specified when the certificate was requested. For more information, see Creating an audit log Certificate Signing Request.

Use these toolbar buttons to manage certificate signing requests.

Table 26: Certificate Signing Request: Toolbar

Option	Description
Delete Signing Request	Delete the selected CSR from SPP.
Refresh	Update the list of CSRs.

Hardware Security Module Certificates

SPP enables an Appliance Administrator to upload both Hardware Security Module client certificates with private keys and Hardware Security Module server certificates for

connecting to Thales Network Luna devices.

Hardware Security Module Client Certificates

Go to Hardware Security Module Client Certificates:

- web client: Navigate to **Certificates** > **Hardware Security Module Certificates** > **Client Certificates**.

To display the following information for the Hardware Security Module client certificate, select a certificate.

Table 27: Client Certificates: Properties

Property	Description
Subject	The name of the subject (such as user, program, computer, service, or other entity) assigned to the certificate when it was requested.
Appliances	Lists the name of the appliance to which the certificate is assigned.
Issued By	The name of the certificate authority (CA) that issued the certificate.
Thumbprint	A unique hash value that identifies the certificate.
Invalid Before	A start date and time that must be met before a certificate can be used.
Expiration Date	The date and time when the certificate expires and can no longer be used.

Use these toolbar buttons to manage Hardware Security Module client certificates.

Table 28: Client Certificates: Toolbar

Option	Description
Add Certificate	Upload a Hardware Security Module client certificate. For more information, see Installing a Hardware Security Module client certificate.
Delete Selected	Delete the selected certificate from SPP.
Assign Certificate to Appliance(s)	Assign the selected certificate to one or more appliances. For more information, see Assigning a Hardware Security Module client certificate.
Unassign Certi-	Unassign the selected certificate from one or more appliances.

Option	Description
ficate from Appliance(s)	
Refresh	Update the list of available Hardware Security Module client certificates.

Hardware Security Module Server Certificates

Go to Hardware Security Module Server Certificates:

- web client: Navigate to **Certificates** > **Hardware Security Module Certificates** > **Server Certificates**.

To display the following information for the Hardware Security Module server certificate, select a certificate.

Table 29: Server Certificates: Properties

Property	Description
Subject	The name of the subject (such as user, program, computer, service, or other entity) assigned to the certificate when it was requested.
Issued By	The name of the certificate authority (CA) that issued the certificate.
Certificate Type	This will be listed as **Unknown**.
Thumbprint	A unique hash value that identifies the certificate.
Invalid Before	A start date and time that must be met before a certificate can be used.
Expiration Date	The date and time when the certificate expires and can no longer be used.

Use these toolbar buttons to manage Hardware Security Module server certificates.

Table 30: Server Certificates: Toolbar

Option	Description
Upload Certificate	Upload a Hardware Security Module server certificate. For more information, see Uploading a Hardware Security Module server certificate.
Delete Selected	Delete the selected certificate from SPP.
Refresh	Update the list of certificates.

Installing a Hardware Security Module client certificate

To install a Hardware Security Module client certificate

1. Go to Client Certificates:
   - web client: Navigate to **Certificates** > **Hardware Security Module Certificates** > **Client Certificates**.
2. Click **Add Certificate**.
3. For **Client Public Key**, click **Upload File**.
4. Select the client certificate public key file and click **Open**.
5. For **Client Private Key**, click **Upload File**.
6. Select the client certificate private key file and click **Open**.
7. On the Add Client Certificate dialog, click **OK**. After the certificate has been uploaded, you need to assign the certificate to one or more appliances. For more information, see Assigning a Hardware Security Module client certificate

Assigning a Hardware Security Module client certificate

SPP allows you to assign Hardware Security Module client certificates that you have previously uploaded to any appliance in your clustered environment.

To assign a client certificate to appliances

1. Go to Client Certificates:
   - web client: Navigate to **Certificates** > **Hardware Security Module Certificates** > **Client Certificates**.
2. Select a certificate and click **Assign Certificate to Appliance(s)**.
3. In the **Assign Certificate to Appliances** dialog, select one or more appliances.
4. Click **OK**.

Uploading a Hardware Security Module server certificate

SPP allows you to upload Hardware Security Module server certificates.

To upload a Hardware Security Module server certificate

1. Go to Server Certificates:
   - web client: Navigate to **Certificates** > **Hardware Security Module Certificates** > **Server Certificates**.
2. Click **Upload Certificate**.
3. Select the server certificate and click **Open**.

SMTP Certificate

Initially, the default self-signed SMTP client certificate used is listed and assigned to the appliance. This default certificate is not a trusted certificate and should be replaced.

Considerations:

- The remote certificate must have a valid CN and/or DNS SAN and it must publish a CRL if the following is true:
  - TLS (STARTTLS or SMTPS) is used with SMTP
  - **Verify SMTP Server Certificate** is selected on **Appliance Management** > **External Integration** > **Email**.
- SPP supports cipher suites for SMTP TLS in both the default mode and the TLS 1.2 mode. For more information, see Cipher support on page 654.
- If a managed domain account is being used for SMTP user authentication, the remote SMTP server must accept the username in the form `user@domain`.

Go to SMTP Certificate:

- web client: Navigate to **Certificates** > **SMTP Certificate**.

The **SMTP Certificate** pane displays the following information for the SMTP client certificates stored in the database.

Table 31: SSL Certificates: Properties

Property	Description
Refresh	Update the list of SMTP client certificates available (uploaded to SPP).
Subject	The name of the subject (such as user, program, computer, service, or other entity) assigned to the certificate when it was requested.
Thumbprint	A unique hash value that identifies the SMTP client certificate.
Add Certificate	Click **Add Certificate** and select one of the following options to replace the default SMTP client certificate with a new certificate:

Property	Description
	• **Install Certificate generated from CSR** • **Install Certificate with Private Key** • **Create Certificate Signing Request (CSR)**
Use Default	Click to return to the SPP default SMTP client certificate.

Creating an SMTP Certificate Signing Request

If you do not want to use a default SMTP client certificate provided with SPP, you can enroll a certificate using a Certificate Signing Request (CSR) to replace the default SMTP client certificate. You can return to the default certificate later.

To create a CSR for a SMTP certificate

1. Go to SMTP Certificate:
   - web client: Navigate to **Certificates** > **SMTP Certificate**.
2. Click the **Add Certificate** button for the certificate to be replaced and select **Create Certificate Signing Request (CSR)**.
3. In the **Certificate Signing Request** dialog, enter the following information:
   a. **Subject (Distinguished Name)**: Enter the distinguished name of the person or entity to whom the certificate is being issued in the proper format like: cn=common name,ou=organizational unit,o=organization. Using the format example, `cn=sam doe,ou=marketing,o=mycompany`. Maximum length is 500 characters.
      - Click **Use Distinguished Name Creator** to create the distinguished name based on your entries in **Fully Qualified Domain Name** (required), **Department**, **Organization**, **City/Locality**, **State/County/Region**, and **Country**.

   b. **Key Size**: Select the bit length of the private key pair. The bit length determines the security level of the SSL certificate. A larger key size is more secure but encryption is slower.
      - 1024
      - 2048 (default)
      - 4096
4. Click **OK** then **Save** to save your selections and enroll the certificate. The certificate is listed in the **SMTP Certificates** pane.

Installing an SMTP certificate

It is recommended that you not use the default SMTP client certificate provided with SPP.

To replace the default SMTP client certificate with your own, the certificate must have the following:

- Enhanced Key Usage extension with the Client Authentication (1.3.6.1.5.5.7.3.2) OID value.
- Key Usage extension with the Digital Signature bit set.

CSRs may be installed in the following formats.

- Install Certificate generated from CSR including:
  - DER Encoded Files (.cer, .crt, or .der)
  - PEM Encoded Files (.pem)
- Install Certificate with Private Key including:
  - PKCS#12 (.p12 or .pfx)
  - Personal Information Exchange Files (.pfx)

To install a SMTP signing certificate

1. Go to SMTP Certificate:
   - web client: Navigate to **Certificates** > **SMTP Certificate**.

   The **SMTP Certificate** pane displays the following information for the SMTP certificates stored in the database.
2. Click the **Add Certificate** button for the SMTP certificate to be replaced. Select the appropriate option:
   - **Install Certificate generated from CSR**
   - **Install Certificate with Private Key**
3. **Browse** to select the certificate file and click **OK**.
4. Once installed, this new certificate will replace the default certificate listed on the **SMTP Certificate** pane.

To use the default certificate

1. To use the default SMTP certificate provided with SPP, go to SMTP Certificate:
   - web client: Navigate to **Certificates** > **SMTP Certificate**.
2. Click the **Use Default** button for the SMTP certificate to be replaced with the default.
3. On the warning **Use Default** dialog, type in the word `Default` to confirm you will be returning to the default certificate.
4. Click **OK**.

SSL/TLS Certificates

SPP enables an Appliance Administrator to upload SSL certificates with private keys or enroll SSL certificates via a CSR.

Initially, the default self-signed SSL certificate used for HTTPS is listed and assigned to the appliance. This default certificate is not a trusted certificate and should be replaced.

Go to the following selection, based on your client:

- web client: Navigate to **Certificates** > **SSL/TLS Certificates**.

To display the following information for the SSL/TLS certificates, select a certificate.

Table 32: SSL Certificates: Properties

Property	Description
Subject	The name of the subject (such as user, program, computer, service, or other entity) assigned to the certificate when it was requested.
Appliances	Lists the name of the appliance to which the certificate is assigned.
Issued By	The name of the certificate authority (CA) that issued the certificate.
Thumbprint	A unique hash value that identifies the certificate.
Alternate DNS Names	Additional or alternate host names (such as, sites or common names) that were specified when the certificate was requested.. For more information, see Creating an audit log Certificate Signing Request on page 177.
Alternate IP Addresses	Additional or alternate host names (such as, IP addresses or common names) that were specified when the certificate was requested. For more information, see Creating an audit log Certificate Signing Request. For the default self-signed SSL certificate, the name and IP address of the appliance is used.
Invalid Before	A start date and time that must be met before a certificate can be used.
Expiration Date	The date and time when the certificate expires and can no longer be used.

Use these toolbar buttons to manage SSL certificates.

Table 33: SSL Certificates: Toolbar

Option	Description
Add Certificate > **Upload Certificate**	Upload an SSL certificate. For more information, see Installing an SSL/TLS certificate on page 189.
Add Certificate > Create Certificate Signing Request (CSR)	Create a CSR to enroll a certificate. For more information, see Creating an SSL/TLS Certificate Signing Request on page 188.
Refresh	Update the list of SSL certificates available (uploaded to SPP).
Assign Certificate to Appliance(s)	Assign the selected certificate to one or more appliances. For more information, see Assigning an SSL/TLS certificate to appliances on page 190.
Unassign Certificate from Appliances	Unassign the selected certificate from one or more appliances.
Delete Selected	Delete the selected certificate from SPP.

Creating an SSL/TLS Certificate Signing Request

When creating a CSR, you uniquely identify the user or entity that will use the requested certificate. SPP allows you to upload or enroll SSL certificates using CSRs. Once uploaded or enrolled, the SSL certificate is added to the SSL certificate store allowing you to assign it to one or more SPP Appliances.

To create a CSR for SSL

1. Go to the following selection, based on your client:
   - web client: Navigate to **Certificates** > **SSL/TLS Certificates**.
2. Click **Add Certificate** and select **Create Certificate Signing Request (CSR)**.
3. In the **Certificate Signing Request** dialog, enter the following information:
   a. **Subject (Distinguished Name)**: Enter the distinguished name of the person or entity to whom the certificate is being issued in the proper format like: cn=common name,ou=organizational unit,o=organization. Using the format example, `cn=sam doe,ou=marketing,o=mycompany`. Maximum length is 500 characters.

- Click **Use Distinguished Name Creator** to create the distinguished name based on your entries in **Fully Qualified Domain Name** (required), **Department**, **Organization**, **City/Locality**, **State/County/Region**, and **Country**.

b. **Subject Alternate Names (DNS)**: Optionally, enter the Data Source Name (DNS) name of the server that will be protected by this certificate. For example, this might be the DNS names of all of the appliances in the SPP cluster.

   If the DNS name changes, you must generate a new certificate.

c. **Subject Alternate Names (IP Address)**: Optionally, enter the IP addresses of the server that will be protected by this certificate. For example, this might be the IP addresses of all the appliances in the SPP cluster.

   If the IP address changes, you must generate a new certificate.

d. **Key Size**: Select the bit length of the private key pair. The bit length determines the security level of the SSL certificate. A larger key size is more secure but encryption is slower.

   - 1024
   - 2048 (default)
   - 4096

4. Click **OK**. You are prompted with a message like: `Please save and submit the following Certificate Signing Request to a Certificate Authority (CA).`
5. Click **Save** to save the CSR to a file. If you do not save the CSR, you will have to generate another one.
6. In the **Certificate Signing Request** pane, click **Refresh** to update the list of certificates added.

Installing an SSL/TLS certificate

To install an SSL/TLS certificate, the certificate must have at least the following:

- Enhanced Key Usage extension with the Server Authentication (1.3.6.1.5.5.7.3.1) OID value.
- Key Usage extension with the Digital Signature bit set.

To install an SSL certificate

1. Go to the following selection:
   - web client: Navigate to **Certificates** > **SSL/TLS Certificates**.
2. Click **+ Add Certificate** and select **Upload Certificate**.
3. **Browse** and select the certificate file then click **Open**.

4. On the dialog box, enter the case sensitive passphrase to import the certificate. If the certificate does not have a private key passphrase, leave the field empty and click **OK**.
5. After the certificate has been uploaded, assign the certificate to one or more appliances. For more information, see Assigning an SSL/TLS certificate to appliances on page 190.

   You may also upload the certificate's root CA to the list of trusted certificates. For more information, see Trusted CA Certificates on page 193.

> **CAUTION: Improper access to the private SSL key could compromise traffic to and from the appliance. For the most secure configuration, create a Certificate Signature Request (CSR) and have it signed by your normal signing authority.**
>
> **Then use the signed request as your SPP SSL Webserver Certificate. This way, no administrator will have access to the private SSL key that is used by SPP and the traffic will be secure.**

Assigning an SSL/TLS certificate to appliances

SPP supports an SSL certificate store that is owned by the cluster. This allows you to assign any SSL certificate that you have previously uploaded or enrolled via CSR to any appliance in your clustered environment.

To assign a certificate to appliances

1. Go to the following selection:
   - web client: Navigate to **Certificates** > **SSL/TLS Certificates**.
2. Select a certificate from the grid and click the **Assign Certificate to Appliance (s)** toolbar button.
3. In the **Appliances** dialog, select one or more appliances and click **OK** to save your selection.

Follow the same steps to **Unassign Certificate** later.

Syslog Client Certificate

An Appliance Administrator can upload a syslog client certificate so that Safeguard for Privileged Passwords can send authenticated messages to syslog servers that do not accept anonymous clients. For more information, see Syslog on page 232.

You can have only one syslog client certificate defined, which is used by all Safeguard for Privileged Passwords Appliances in the same cluster.

Instead of using the default syslog client certificate supplied, it is recommended you generate the Certificate Signing Request (CSR) using **Create Certificate Signing Request (CSR)**. For more information, see Creating a syslog client Certificate Signing Request on page 192.

If you do use the default syslog client certificate, you are responsible for configuring the syslog server to accept the default certificate. For more information, see Installing a syslog client certificate on page 192.

Manage a Certificate Signing Request (CSR)

To define, generate, or manage a syslog client certificate, go to Syslog Client Certificate:

- web client: Navigate to **Certificates** > **Syslog Client Certificate**.

The following properties and controls are available to manage your syslog client certificate.

Table 34: Syslog Client Certificate: Properties

Property	Description
Refresh	Click to get the latest information about the client certificate used.
Subject	Displays the client which is the name of the subject assigned to the certificate when it was requested.
Thumbprint	A unique hash value that identifies the certificate.
Expiration Date	The expiration date of the certificate.
Add Certificate	Click **Add Certificate** and select one of the following options to replace the default certificate with a new certificate: • **Install Certificate generated from CSR**: For more information, see Installing a syslog client certificate on page 192. • **Install Certificate with Private Key**: For more information, see Installing a syslog client certificate on page 192. • **Create Certificate Signing Request (CSR)**: For more information, see Creating a syslog client Certificate Signing Request on page 192.
Use Default	Click **Use Default** to reset the certificate back to the default supplied by SPP. By default, the data is encrypted in transit but there is no authentication of the client/server.

Creating a syslog client Certificate Signing Request

A certificate signing request (CSR) is submitted to a Certificate Authority (CA) to obtain a digitally signed certificate. When creating a CSR, you uniquely identify the user or entity that will use the requested certificate. SPP allows you to upload or enroll a syslog client certificate using CSRs. Once uploaded or enrolled, the syslog client certificate is added to the syslog client certificate store allowing you to assign it to one or more SPP Appliances.

To create a CSR for syslog

1. Go to the following selection, based on your client:
   - web client: Navigate to **Certificates** > **Syslog Client Certificate**.
2. Click **Add Certificate** and select **Create Certificate Signing Request (CSR)**.
3. In the **Certificate Signing Request** dialog, enter the following information:
   a. **Subject (Distinguished Name)**: Enter the distinguished name of the person or entity to whom the certificate is being issued in the proper format like: cn=common name,ou=organizational unit,o=organization. Using the format example, `cn=sam doe,ou=marketing,o=mycompany`. Maximum length is 500 characters.
      - Click **Use Distinguished Name Creator** to create the distinguished name based on your entries in **Fully Qualified Domain Name** (required), **Department**, **Organization**, **City/Locality**, **State/County/Region**, and **Country**.

   b. **Key Size**: Select the bit length of the private key pair. The bit length determines the security level of the SSL certificate. A larger key size is more secure but encryption is slower.
      - 1024
      - 2048 (default)
      - 4096
4. Click **OK** to save your selections and enroll the certificate.

Installing a syslog client certificate

To install a syslog client certificate, the certificate must have at least the following:

- Enhanced Key Usage extension with the Client Authentication (1.3.6.1.5.5.7.3.2) OID value.
- Key Usage extension with the Digital Signature bit set.

To install a syslog client certificate

1. Go to the following:
   - web client: Navigate to **Certificates** > **Syslog Client Certificate**.
2. Click **Add Certificate** and select one of the following:
   - **Install Certificate with a Private Key**: To upload a PFX file that contains the certificate and the private key
   - **Install Certificate generate from CSR**: To generate a CSR and have that signed by a trusted CA
3. **Browse** to select the certificate file and complete the install.
4. For **Enter the private key passphrase**:
   - Enter the passphrase to import the certificate then click **OK**. Click to see the passphrase.
   - If there is no passphrase, leave the field blank then click **OK**.
5. The **Subject**, **Thumbprint**, and **Expiration** date for the key you uploaded displays. You can select **Use Default** and respond to the confirmation dialog to return to the default, if desired.
6. If you uploaded a certificate with a private key, you may upload the certificate's root CA to the list of trusted certificates. For more information, see Trusted CA Certificates on page 193.

Trusted CA Certificates

It is the responsibility of the Appliance Administrator to add or remove trusted root certificates to the Safeguard for Privileged Passwords Appliance. If you are going to verify the server certificate, then you do need a certificate from the server certificates chain of trust in Trusted Certificates.

Examples:

- If you uploaded a syslog client certificate with a private key, you may need to upload the certificate's root CA to the list of trusted certificates. For more information, see Syslog Client Certificate on page 190.
- An SSL/TLS certificate must be trusted to resolve the chain of authority. For an SSL/TSL certificate, when Safeguard for Privileged Passwords connects to an asset that has the **Verify SSL Certificate** option enabled, the signing authority of the certificate presented by the asset is compared to the certificates in the trusted certificate store. For more information, see Directory Account, *Verify SSL Certificate*.

Go to the following:

- web client: Navigate to **Certificates** > **Trusted CA Certificates**.

Select a certificate to display the following information for the user-supplied certificates added to the trusted certificate store.

Table 35: Trusted CA certificates: Properties

Property	Description
Subject	The name of the subject (such as user, program, computer, service or other entity) assigned to the certificate when it was requested.
Issued By	The name of the certificate authority (CA) that issued the certificate.
Certificate Type	Trusted
Thumbprint	A unique hash value that identifies the certificate.
Invalid Before	A "start" date and time that must be met before a certificate can be used.
Expiration Date	The date and time when the certificate expires and can no longer be used.

Toolbar options follow.

Table 36: Trusted Certificates: Toolbar

Option	Description
Upload New Trusted CA Certificate	Add a trusted certificate.
Delete Selected	Delete the selected certificate.
Refresh	Update the list of certificates.

Adding a trusted certificate

Prior to adding an asset that uses SSL server certificate validation, add the certificate's root CA and any intermediate CAs to the Trusted Certificates store in SPP. For more information, see Verify SSL Certificate.

You may need to add the syslog server certificate if it is signed by the same CA.

If a certificate upload fails, the audit log reflects: `TrustedCertificateUploadFailed` or `ServerCertificateUploadFailed`.

To add a trusted certificate

1. Go to the following:
   - web client: Navigate to **Certificates** > **Trusted CA Certificates**.
2. Click **+ Upload New Trusted CA Certificate** from the details toolbar.
3. **Browse** and select the certificate file then click **Open**.
4. On the dialog box, enter the case sensitive passphrase to import the certificate. If the certificate does not have a private key passphrase, leave the field empty and click **OK**.

Removing a trusted certificate

To remove certificates from the appliance

1. Go to the following:
   - web client: Navigate to **Certificates** > **Trusted CA Certificates**.
2. Select a certificate.
3. Click **Delete Trusted CA Certificate** from the details toolbar.

   IMPORTANT: SPP does not allow you to remove built-in certificate authorities.

Cluster

Use the Cluster settings to create a clustered environment, to monitor the health of the cluster and its members, and to define managed networks for high availability and load distribution.

It is the responsibility of the Appliance Administrator or the Operations Administrator to create a cluster, monitor the status of the cluster, and define managed networks.

Before creating a SPP cluster, become familiar with the Disaster recovery and clusters chapter to understand:

- Primary and replica appliances
- Consensus
- Supported clusters in SPP
- Ports
- Offline Workflow to automatically or manually enable access request, approval, and release in the event an appliance loses consensus with the cluster (for example, by losing connectivity or availability): Manually control Offline Workflow Mode.
- Enrollment into a cluster: Enrolling replicas into a cluster

- Recover a cluster that has lost consensus: For more information, see Resetting a cluster that has lost consensus on page 593.

Go to the following:

- web client: Navigate to **Cluster**.

Table 37: Cluster settings

Setting	Description
Cluster Management	Where you create and manage a cluster and monitor the health of the cluster and its members.
Managed Networks	Where you define managed networks to distribute the task load for the clustered environment.
Offline Workflow (automatic)	Where you configure Offline Workflow Mode to automatically trigger if an appliance has lost consensus (quorum) and, optionally, automatically resume online workflow. You can also manually **Enable Offline Workflow** and **Resume Online Operations** from this dialog. For more information, see About Offline Workflow Mode on page 581.
Session Appliances with Safeguard for Privileged Sessions link	Where you view, edit, and delete link connections when a Safeguard for Privileged Sessions cluster is linked to a Safeguard for Privileged Password for session recording and auditing. For more information, see SPP and Safeguard for Privileged Sessions appliance link guidance on page 684.

Cluster Management

Cluster Management allows you to create and diagnosis clusters.

When using Cluster Management from the web client, performing operations against other members of the cluster will incur a Cross-Origin Resource Sharing (CORS) HTTP request. This may require you to change the Trusted Servers, CORS, and Redirects setting to allow the specific host name being used in your web browser.

Navigate to **Cluster** > **Cluster Management**.

Cluster Management grid

- Health indicators: Health indicators display in the first column in the Cluster Management grid. Cluster members periodically query other appliances in the cluster to obtain their health information. Cluster member information and health information is cached in memory, with the most recent results displayed.

  The health indicators on the nodes indicate if cluster members are in any of these states:

  error: Indicates a definite problem impacting the functionality of the cluster

warning: Indicates a potential issue with the cluster

locked: Indicates the cluster is locked

(green) healthy state.

Expand the **View More** section to see more details.

- **Name**: The name of the appliance.
- **Network Address**: The IPv4 address (or IPv6 address) of the appliance configuration interface. You can modify the appliance IP address. For more information, see How do I modify the appliance configuration settings on page 664.
- **Primary**: Displays **Yes** if the appliance is the primary.
- **Appliance State**: Indicates the appliance state. For a list of available states, see Appliance states.

When you select an appliance, the details for the appliance display on the right. The grid information displays: name, network address, primary, and state. This additional information is available:

- **Disk Space**: The amount of used and free disk space.
- **Version**: The appliance version number.
- **Last Health Check**: Last date and time the selected appliance's information was obtained.
- **Uptime**: The amount of time (days, hours, and minutes) the appliance has been running.
- If the replica is selected, this additional information displays for the **Primary**:
  - **Network Address**: The network DNS name or the IP address of the primary appliance in the cluster
  - **MAC Address**: The media access control address (MAC address), a unique identifier assigned to the network interface for communications
  - **Link Present**: Displays either Yes or No to indicate if there is an open communication link
  - **Link Latency**: The amount of time (in milliseconds) it takes for the primary to communicate with the replica. Network latency is an expression of how much time it takes for a packet of data to get from one designated point to another. Ideally, latency is as close to zero as possible.
- Errors and warnings are reported:
  - **Errors**: Errors are reported. For example, if an appliance is disconnected from the primary (no quorum), an error message may be: `Request Workflow: Cluster configuration database health could not be determined.`
  - **Warnings**: Warnings are reported. For example, if an appliance is disconnected from the primary (no quorum), a warning message may be: `Policy Data: There is a problem replicating policy data. Details:`

```
Policy database slave IO is not running. The Safeguard primary may be
inaccessible from this appliance.
```

Toolbar actions

- **Add Replica**: Join an appliance to the primary appliance as a replica. For more information, see Enrolling replicas into a cluster on page 577.
- Appliance details and cluster health pane toolbar buttons follow.
  - **Unjoin**: Click **Unjoin** to remove a replica from the cluster. For more information, see Unjoining replicas from a cluster on page 578.
  - **Failover**: Click **Failover** to promote a replica to the primary appliance. For more information, see Failing over to a replica by promoting it to be the new primary on page 587.
  - **Activate**: Click **Activate** to activate a read-only appliance so it can add, modify and delete data. For more information, see Activating a read-only appliance on page 588.

    CAUTION: Activating an appliance that is in Read-Only mode will take it out of the Read-only state and enable password and SSH key check and change for managed accounts. Ensure that no other SPP Appliance is actively monitoring these accounts, otherwise access to managed accounts could be lost.

  - **Diagnose**: Click **Diagnose** to open the Diagnostics pane where you can perform the following:
    - View appliance diagnostics. For more information, see Appliance Diagnostics on page 126.
    - View appliance information. For more information, see Appliance Information on page 127.
    - Run diagnostic tests against the appliance. For more information, see Network Diagnostics on page 137.
    - View or edit networking settings. For more information, see Networking on page 141.
    - Perform a factory reset. For more information, see Factory Reset on page 133.
    - Check OS licensing (virtual machine only). For more information, see Operating System Licensing on page 144.
    - Update patches. For more information, see Patch Updates on page 146.
    - Power down and restart the appliance. For more information, see Power on page 147.
    - Generate a support bundle. For more information, see Support bundle

on page 148.

- View or edit time settings. For more information, see Time on page 149.

- **Check Health**: Click **Check Health** to capture and display the current state of the selected appliance.

- **Restart**: Click **Restart** to restart the selected appliance. Confirm your intentions by entering a **Reason** and clicking **Restart**.

- **Reset Cluster**: Reset a cluster to recover a cluster that has lost consensus. For more information, see Resetting a cluster that has lost consensus on page 593.

  CAUTION: Resetting a cluster should be your last resort. It is recommended that you restore from a backup rather than reset a cluster.

- **Refresh**: Update the list of appliances in a cluster.
- **Enable Offline Workflow**: This button is available if the appliance has lost consensus, you are logged into the selected appliance, and you have not already put the appliance in Offline Workflow Mode. The state of the appliance will be `Isolated` or `Lost Quorum`.
  Click **Enable Offline Workflow** to manually place the selected appliance in Offline Workflow Mode. The appliance will run in isolation from the rest of the cluster. For more information, see Manually control Offline Workflow Mode on page 585.
- **Resume Online Operations**: This button is available if the appliance has lost consensus, you are logged into the selected appliance, and the appliance is in Offline Workflow Mode. The state of the appliance will be `Isolated` or `Lost Quorum`.
  Click **Resume Online Operations** to manually reintegrate the appliance with the cluster and merge audit logs. For more information, see To manually resume online operations on page 586.

Related Topics

- Task delegation in a cluster
- Password distribution in a cluster

Unlocking a locked cluster

In order to maintain consistency and stability, only one cluster operation can run at a time. To ensure this, SPP locks the cluster while a cluster operation is running, such as enroll, unjoin, failover, patch, reset, session module join, update IP, and audit log maintenance. While the cluster is locked, changes to the cluster configuration are not allowed until the operation completes.

The lock notification displays as follows:

- web client: The **Appliance State** will show a red lock icon ( ).

You should never cancel the cluster lock for an SPP unjoin, failover, cluster reset, restore, patch, or IP address update. Other considerations:

- If a SPP join (enroll) is taking a long time, you may cancel it during the streaming audit data step.
- If a patch distribution is taking a long time, you may cancel it and upload the patch to the replicas directly.
- If an audit log synchronize operation is taking a long time, or you have reason to believe it will not complete due to a down appliance in the cluster, you may cancel it. Canceling this operation requires monitoring as detailed in Cancel Audit Log Maintenance from the Audit Log Maintenance page.
- If an audit log archive or purge operation is taking a long time, or you have reason to believe it will not complete due to a down appliance in the cluster, you may cancel it. Canceling this operation requires monitoring as detailed in Cancel Audit Log Maintenance from the Audit Log Maintenance page.

To unlock a locked cluster

1. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
2. Click the lock icon in the upper right corner of the warning banner.
3. In the **Unlock Cluster** confirmation dialog, enter **Unlock Cluster** and click **OK**.

   This will release the cluster lock that was placed on all of the appliances in the cluster and close the operation.

IMPORTANT: Care should be taken when unlocking a locked cluster. It should only be used when you are sure that one or more appliances in the cluster are offline and will not finish the current operation. If you force the cluster unlock, you may cause instability on an appliance, requiring a factory reset and possibly the need to rebuild the cluster. If you are unsure about the operation in progress, do NOT unlock the cluster.

Task delegation in a cluster

A Safeguard for Privileged Passwords' cluster delegates platform management tasks (such as password and SSH key check and password and SSH key change) to appliances based on platform task load. The primary appliance performs delegation and evaluates cluster member suitability using an internal fitness score that is calculated by dividing the number of in-use platform task threads by the maximum number of allowed platform task threads.

The maximum number of allowed platform task threads can be adjusted using the Appliance/Settings API and adjusting the `MaxPlatformTaskThreads` value. By adjusting this number, you can tune task distribution.

IMPORTANT: Adjusting the `MaxPlatformTaskThreads` will impact SPP's available resources for handling access requests and may impact user experience. Best practice is to engage Professional Services if the value may need to be changed.

Increasing the maximum number of allowed platform task threads will decrease the fitness score thus increasing the number of tasks passed to that appliance.

The fitness score is cached and is recalculated in 8-minute intervals when the scheduler is not busy. When the scheduler is running tasks, the fitness score is calculated more frequently so the scheduler can dynamically adjust.

The selection of a Safeguard for Privileged Sessions Appliance is primarily dependent on managed network rules. However, if there aren't any managed network rules or if the managed network rules result in more than one Safeguard for Privileged Sessions appliances selected, a fitness score is used as the tie breaker. The fitness score is calculated based on the percentage of disk available minus the overall load average of the Safeguard for Privileged Sessions appliance. (Load average is a Linux metric which provides a numerical indication of the overall resource capacity in use on the server.) The higher the fitness score, the more likely that the corresponding appliance will be selected.

Password distribution in a cluster

The Primary coordinates all password changes across the cluster. When the scheduler decides it is time to change a password, it will choose whichever node is least busy (based on a fitness score and part of the Managed Network) and assign the task to that cluster member. When the cluster member is done and the change is successful, the password change is written immediately from that replica into the distributed database. It has consensus (quorum) which means that all nodes that are part of that quorum will immediately receive the password.

The same is true for a session. If the Primary schedules a password change, and someone attempts to use a session, it should have the correct password.

There is a potential scenario where the password or session request has already been initiated and the Primary schedules a change during the request. In this case, the user will have to check out the password anew, but an existing session that is live should not be interrupted. If they attempt to initiate the session at the exact moment that the password change has happened, they may get an error about the session.

Password distribution changes when Offline Workflow is enabled on a node that has lost consensus (quorum). For more information, see About Offline Workflow Mode.

Managed Networks

Managed networks are named lists of network segments serviced by a specific SPP (SPP) or Safeguard for Privileged Sessions (SPS) appliance in a clustered environment. Managed networks are used for scheduling tasks, such as password or SSH key change, account discovery, sessions recording, and asset discovery to distribute the task load. Using managed networks, you can:

- Distribute the load so there is minimal cluster traffic.
- Specify to use the appliances that are closest to the target asset to perform the actual task.

A SPP cluster has a default managed network that consists of all cluster members. Other managed networks can be defined.

> **CAUTION: If the role of a managed host that belongs to a linked Safeguard for Privileged Sessions cluster is changed or if a managed host is added or removed from the cluster, SPP will detect the change by querying each Central Management node and attempt to stay in sync with the Safeguard for Privileged Sessions cluster topology. If the Central Management node is down, SPP warns the administrator there may be invalid policies with a message like:** `The session connection policy was not found`**, in addition to flagging each broken Access Request Policy with an Invalid notation (Security Policy Management > Entitlements > Access Request Policies tab). Based on the size of your network and other factors, this will take one to 10 minutes and, during this time window, an unavailable managed host may continue to appear on the Managed Networks page. Any requests made will be invalid and will not be able to be launch sessions.**

Precedence

The selection made on the **Entitlement** > **Access Request Policy** tab takes precedence over the selections on **Appliance Management** > **Cluster** > **Managed Networks** page. If a **Managed Networks** rule includes nodes from different Safeguard for Privileged Sessions clusters, Safeguard for Privileged Passwords will only select the nodes from the same cluster that was assigned on the **Session Settings** page of the **Access Request Policy** tab.

> IMPORTANT: Discovery, password and SSH key check and change will not work if a managed network has been configured with a subnet but is not assigned to an appliance (the appliance is blank). If the managed network does not have an assigned appliance, a message like the following displays: `No appliances in network '<NameOfEmptyNetwork>' available to execute platform task request`. To resolve the issue, assign at least one appliance to manage the passwords, SSH key, and/or sessions or delete the managed network entry.

Go to Managed Networks:

- web client: Navigate to **Appliance Management** > **Cluster** > **Managed Networks**.

The **Managed Networks** page displays the following information about previously defined managed networks. Initially, this page contains the properties for the Default Managed Network, which implicitly includes all networks and is served by all appliances in the cluster.

Table 38: Managed Networks: Properties

Property	Description
Name	The name assigned to the managed network when it was added to SPP.

Property	Description
Subnets	A list of subnets included in the managed network. Double-click an entry in the Managed Networks grid to display details about the subnets associated with the selected managed network. If you have linked Safeguard for Privileged Sessions, the following apply: • **Passwords Managed By**: The SPP appliance ID, which includes the MAC address followed by the IP address of the node. • **Sessions Managed By**: If applicable, the Safeguard for Privileged Sessions appliance host name followed by the IP address of the Safeguard for Privileged Sessions node.
Passwords Managed By	The host name and IP address of the appliances and the MAC address assigned to manage the specified subnets.
Sessions Managed By	The host name and IP address of the cluster nodes.
Description	The descriptive text entered when defining the managed network.

Use these toolbar buttons to define and maintain your managed networks.

Table 39: Managed Networks: Toolbar

Option	Description
New	Add a managed network. For more information, see Adding a managed network on page 204.
Delete Selected	Remove the selected managed network from SPP. You cannot delete the Default Managed Network.
Refresh	Update the list of managed networks.
Edit	Modify the selected managed network configuration. You can not modify the Default Managed Network.
Resolve Network text box	Locate an IP address in a managed network's list of subnets. For more information, see Resolving IP address on page 205.

Related Topics

- Task delegation in a cluster
- Password distribution in a cluster

Adding a managed network

Use the **Managed Networks** page on the Cluster settings view to add managed networks, which can be used to distribute the task load in a clustered environment. It is the responsibility of the Appliance Administrator to define and maintain managed networks.

To add a managed network

1. Go to Managed Networks:
   - web client: Navigate to **Cluster** > **Managed Networks**.
2. Click **+ Add**.
3. In the **Managed Network** dialog, provide the following information:
   a. **Name**: Enter the display name for the managed network. This may be the name of the Safeguard for Privileged Sessions Appliance used to authenticate the linked Safeguard for Privileged Sessions session connection.

      Limit: 50 characters

   b. **Description**: (Optional) Enter information about the managed network.

      Limit: 255 characters

   c. **Subnets**: Click **+Add** to specify the subnets, or group of hosts, to be managed.

      Enter each subnet using CIDR notation. For example, 0.0.0.0/0.

      > NOTE: You can add a subnet to only one managed network. You will receive an error if you attempt to add the same subnet to another managed network. If you are unsure if an IP address has already been associated with a managed network, use the **Resolve Network** search box. For more information, see Resolving IP address on page 205.

   d. **Passwords Managed By**: Select the appliances to be used to manage the specified subnets.

      > NOTE: You do not need to specify an appliance when you initially define a managed network. You can use the **Edit** button to specify the managing appliance at a later time.

   e. **Sessions Managed By**: If applicable, select the Safeguard for Privileged Sessions appliance to associate with the managed network.
4. Click **OK** to save your selections and add the managed network.

Deleting a managed network

To delete a managed network

1. Go to Managed Networks:
   - web client: Navigate to **Cluster** > **Managed Networks**.
2. Select the managed network to be deleted, click **Delete**.
3. In the confirmation dialog, click **Yes**.

Resolving IP address

As an Appliance Administrator, you can use the **Managed Networks** page to search for an IP address within a managed network's list of subnets.

To find an IP address in a managed network

1. Go to Managed Networks:
   - web client: Navigate to **Cluster** > **Managed Networks**.
2. In the **Resolve Network** search box, type the IP address, and press **Enter**.

   The managed network that contains the subnet that most closely matches the IP address is highlighted. If there are no subnets that match the IP address, the Default Managed Network is highlighted.

Offline Workflow (automatic)

To reduce potential downtime, the Appliance Administrator can configure Offline Workflow Mode to be performed automatically. Offline Workflow Mode allows an appliance that has lost consensus (quorum) to operate in isolation from the cluster to process access requests using cached policy data.

To ensure the outage is not a short-lived outage, the default time before the appliance is automatically switched to Offline Workflow Mode is 15 minutes. The time threshold can be changed to five minutes or more.

If automatic Offline Workflow Mode is enabled, you can enable automatic Resume Online Workflow so the appliance automatically resumes online operations once consensus is restored. The minutes to wait after consensus is restored before automatically resuming online workflow defaults to 15 minutes. The time threshold can be changed to five minutes or more.

When Offline Workflow Mode settings are configured to run automatically, an Appliance Administrator can override the automatic settings and manually place an appliance in Offline Workflow Mode or manually restore an appliance to online workflow, as needed.

The user views status messages that clearly communicate the appliance state and the ability to request passwords and SSH keys.

For general information on Offline Workflow Mode, see About Offline Workflow Mode.

Go to Offline Workflow:

- web client: Navigate to **Cluster** > **Offline Workflow**.

The **Offline Workflow** page displays the following information.

Table 40: Offline Workflow: Properties

Property	Description
Enable Automatic Offline Workflow	To automatically place the appliance in Offline Workflow Mode when the appliance loses connection and cannot establish consensus.
Automatic Offline Workflow Threshold Minutes	The number of minutes after consensus is lost before the appliance is automatically switched over to Offline Workflow Mode. The default is 15 minutes and can be changed to five minutes or more. The threshold set does not persist after a reboot.
Automatic Resume Online Workflow	If you selected **Enable Automatic Offline Workflow**, you can select **Automatic Resume Online Workflow** so the appliance automatically resumes online operations once consensus is restored.
Automatic Resume Online Workflow Threshold	The number of minutes after consensus is restored that the appliance is automatically switched over to online workflow. The default is 15 minutes and can be changed to five minutes or more.

Use these toolbar buttons to define and maintain your managed networks.

Table 41: Offline Workflow: Toolbar

Option	Description
Refresh	Updates the information displayed on the page
Enable Offline Workflow	Triggers Offline Workflow Mode
Resume Online Operations	Triggers moving the appliance from Offline Workflow Mode back to online operations

Enable automatic Offline Workflow

Use the **Offline Workflow** page to configure automatic settings to control Offline Workflow Mode. You can manually override the automatic settings. For more information, see Manually override automatic Offline Workflow on page 207.

To configure automatic settings to control Offline Workflow Mode

1. Go to Offline Workflow:
   - web client: Navigate to **Cluster** > **Offline Workflow**.
2. On the **Offline Workflow** dialog, select **Enable Automatic Offline Workflow** so the appliance will be automatically placed in Offline Workflow Mode when the appliance loses connection and cannot establish consensus with the cluster for the specified number of minutes entered (see next step).
3. Identify the number of **Minutes** after consensus is lost before the appliance is automatically switched over to Offline Workflow Mode. The **Automatic Offline Workflow Threshold** defaults to 15 minutes and can be changed to a minimum of five minutes or more.
4. If you selected the first check box to enabled automatic Offline Workflow Mode, you can select **Automatic Resume Online Workflow** so the appliance automatically resumes online operations once consensus with the cluster is restored for the specified number of minutes entered (see next step).
5. Identify the number of **Minutes** after consensus is restored that the appliance is automatically switched over to online workflow. The **Automatic Resume Online Workflow Threshold** defaults to 15 minutes and can be changed to a minimum of five minutes or more.
6. Click **Save**.

Manually override automatic Offline Workflow

Use the **Offline Workflow** page to manually enable offline workflow or resume online operations.

For details on either of these operations, see Manually control Offline Workflow Mode.

Before resuming online operations, see Considerations to resume online operations.

To manually Enable Offline Workflow

This option is only available when the appliance has lost consensus with the cluster.

1. Go to Enable Offline Workflow:
   - web client: Navigate to **Cluster** > **Offline Workflow**.
2. Click **Enable Offline Workflow** to manually trigger Offline Workflow Mode.

3. In the dialog box, type in **Enable Offline Workflow** and click **Enter**. The appliance is in Offline Workflow Mode and enters maintenance.
4. You can verify requests and view health checks on the **Cluster Management** window. For more information, see Cluster Management on page 196.

To manually Resume Online Operations

This option is only available when the appliance is in Offline Workflow Mode.

1. Go to Offline Workflow:
   - web client: Navigate to **Cluster** > **Offline Workflow**.
2. Click **Resume Online Operations** to manually trigger moving the appliance from Offline Workflow Mode back to online operations.
3. In the dialog box, type in **Resume Online Operations** and click **Enter.**
4. When maintenance is complete, select to restart. The appliance is returned to Maintenance mode.
5. You can verify requests and view health checks on the **Cluster Management** window. For more information, see Cluster Management on page 196.

Session Appliances with Safeguard for Privileged Sessions link

The Asset Administrator can link a Safeguard for Privileged Sessions (SPS) cluster to a SPP (SPP) cluster of one appliance or more for session recording and auditing. The actual link must be between the SPP primary and the Safeguard for Privileged Sessions cluster master. This means that the Safeguard for Privileged Sessions cluster is aware of each node in an SPP cluster and vice-versa.

Once linked, all sessions are initiated by the SPP appliance via an access request and managed by the Safeguard for Privileged Sessions appliance and sessions are recorded via the Sessions Appliance.

CAUTION: When linking your Safeguard for Privileged Sessions (SPS) deployment to your SPP (SPP) deployment, ensure that the SPS and SPP versions match exactly, and keep the versions synchronized during an upgrade. For example, you can only link SPS version 6.6 to SPP version 6.6, and if you upgrade SPS to version 6.7, you must also upgrade SPP to 6.7.

Make sure that you do not mix Long Term Supported (LTS) and feature releases. For example, do not link an SPS version 6.0.1 to an SPP version 6.1.

NOTE: If you have a single node Safeguard for Privileged Sessions cluster where the Central Management node is also the Search Master, SPP will be unable to launch sessions. There has to be at least one Safeguard for Privileged Sessions appliance in the

cluster that is capable of recording sessions. See the *One Identity Safeguard for Privileged Sessions Administration Guide*, Managing Safeguard for Privileged Sessions (SPS) clusters.

Safeguard for Privileged Passwords link guidance

Before initiating the link, review the steps and considerations in the link guidance. For more information, see For more information, see SPP and Safeguard for Privileged Sessions appliance link guidance on page 684..

Pay attention to the roles assigned to the SPS nodes. The following caution is offered to avoid losing session playback from SPP.

CAUTION: Do not switch the role of a Safeguard for Privileged Sessions node from the Search Local role to Search Minion role. If you do, playback of the sessions recorded while in the Search Local role may not be played back from the SPP appliance, and may only be played back via the Safeguard for Privileged Sessions web user interface. Recordings made with the node in Search Minion role are pushed to the Search Master node and are available for download to SPP. For details about Safeguard for Privileged Sessions nodes and roles, see the *One Identity Safeguard for Privileged Sessions Administration Guide*: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Standard operating procedure after the initial link

If you add another Safeguard for Privileged Sessions cluster after the initial link, follow these standard operating procedures:

1. Add link connections. See Viewing, deleting, or editing link connections.
2. Identify the session settings on the entitlements access request policy (**SPS Connection Policy** which is the IP address of the cluster master). For more information, see Creating an access request policy
3. Assign the managed networks. For more information, see For more information, see Managed Networks on page 201..
4. Enable the **Session Access Enabled** toggle.

If the Safeguard for Privileged Sessions Central Management node is down

SPP continues to launch sessions on the managed hosts when the Safeguard for Privileged Sessions Central Management node is down. However, as long as the Central Management node is down, SPP cannot validate existing policies nor can it validate the Safeguard for Privileged Sessions cluster topology. For more information, see *Managing a High Availability One Identity Safeguard for Privileged Sessions (SPS) cluster* in the *One Identity Safeguard for Privileged Sessions Administration Guide*.

Viewing, deleting, or editing link connections

Once the link is complete, in the web client, navigate to go to **Cluster** > **Session Appliances**.

The **Session Appliances** pane displays the following session details.

Table 42: Session Appliances: Properties

Property	Description
Host Name	The host name of the Safeguard for Privileged Sessions appliance host cluster master.
Managed Hosts	Other nodes in the Safeguard for Privileged Sessions cluster identified by the managed host name and IP address. Hover over any ⚠ **Warning** icon to see if the **Managed Host** is **Unavailable** or **Unknown**.
Network Address	The network DNS name or IP address of the session connection.
Connection User	The user name for Safeguard for Privileged Passwords. Do not include spaces in the user name.
Thumbprint	A unique hash value that identifies the certificate.
Description	(Optional) Descriptive text about the Safeguard for Privileged Sessions session connection (for example, 20 on cluster - 172 primary node).

Double-click a **Host Name** row to bring up the **Session Module Connection** dialog.

Table 43: Session Module Connection: Properties

Property	Description
Node ID	The name of the Safeguard for Privileged Sessions Appliance used to authenticate the linked SPS session connection.
Host Name	The host name of the Safeguard for Privileged Sessions appliance host cluster master.
Connection User name	The user name for Safeguard for Privileged Passwords. Do not include spaces in the user name.
Description	(Optional) Descriptive text about the Safeguard

Property	Description
	for Privileged Sessions session connection (for example, 20 on cluster - 172 primary node).
Network Address	The network DNS name or IP address of the session connection.
Use Host Name For Launch (not IP address)	If checked, the connection string used to launch a session uses the host name of the Safeguard for Privileged Sessions appliance rather than the IP address.

Use these toolbar buttons to manage sessions.

Table 44: Sessions Management: Toolbar

Option	Description
Remove	Remove the selected linked Safeguard for Privileged Sessions session connection. For details on soft versus hard deletes, see Connection deletion: soft delete versus hard delete.
Edit	Modify the selected linked Safeguard for Privileged Sessions session connection **Description** or **Network Address** on the **Session Module Connection** dialog.
Refresh	Update the list of linked Safeguard for Privileged Sessions session connections.

Connection deletion: soft delete versus hard delete

Depending on your goals, you can perform a soft delete or a hard delete.

Soft delete the connection

When a session connection is deleted, the connection information is soft deleted so that a relink of the same Safeguard for Privileged Sessions appliance can reuse the same values. This approach of soft deleting and reusing the same connection values on a relink avoids "breaking" all of the Access Request Polices that referenced the previous session connection.

Hard delete the connection

A hard delete can be performed to permanently remove the session connection. This is usually only done in cases where either a relink is not desired or retaining the previous

session connection values is preventing a Safeguard for Privileged Sessions appliance from linking or relinking.

A hard delete can be performed from the API using the following steps for using PowerShell or Swagger.

Hard delete with PowerShell

The latest version of Safeguard PowerShell includes two cmdlets to perform the hard delete:

```
split-safeguardSessionCluster -SessionMaster <name or ID of session master>
```

```
Remove-SafeguardSessionSplitCluster -SessionMaster <name or ID of session master>
```

For more information, see OneIdentity/safeguard-ps.

Hard delete with Swagger

To perform hard deletion with Swagger

1. In a browser, navigate to `https://<your-ip-address>/service/core/swagger`.
2. Authenticate to the service using the **Authorize** button.
3. Navigate to `Cluster->GET /v4/cluster/SessionModules` and click **Try it out!**.
4. Identify if the unwanted session connection exists on the list:
   a. If the unwanted session connection exists in the list, then:
      i. Note the ID of the session connection.
      ii. Navigate to `Cluster DELETE /v4/cluster/SessionModules`.
      iii. Enter the ID.
      iv. Click **Try it out!**.
      v. Go to step 3.
   b. If the unwanted session connection does not exist in the list, then:
      i. Set the `includeDisconnected` parameter to true.
      ii. Click **Try it out!**.
      iii. If the unwanted session connection exists in the list, then go to step 4a to delete the entry a second time which will result in a hard delete.
5. The process is complete and the session connection is permanently removed.

Global Services

One Identity Safeguard for Privileged Passwords allows you to enable or disable SPP services from the **Global Services** page.

By default, services are disabled for service accounts and for accounts and assets found as part of a discovery job. Service accounts can be modified to adhere to these schedules and discovered accounts can be activated when managed.

It is the responsibility of the Appliance Administrator to manage these settings.

Navigate to **Global Services** to see the settings listed below.

- Appliance Administrators can click the **Disable All** button to disable all services (as long as at least one service is currently enabled). A dialog will appear asking for confirmation before disabling the services.
- Click a toggle to change a setting: toggle on and toggle off.
- Click **Refresh** to update the information on the page.

Table 45: Global Services settings

Setting	Description
Disable All	Appliance Administrators can use this button to disable all services (as long as at least one service is currently enabled). A dialog will appear asking for confirmation before disabling the services. You will need to reenable each service individually.
Requests	
Session Requests	Session requests are enabled by default, indicating that authorized users can make session access requests. There is a limit of 1,000 sessions on a single access request. Click the **Session Requests** toggle to disable this service so sessions can not be requested. NOTE: When Session Requests is disabled, no new session access requests can be initiated. Depending on the access request policies that control the target asset/account, you will see a message informing you that the Session Request feature is not available. In addition, current session access requests cannot be launched. A message appears, informing you that Session Requests is not available. For example, you may see the following message: `This feature is temporarily disabled. See your appliance administrator for details.`
Password Requests	Password requests are enabled by default, indicating that authorized users can make password release requests Click the **Password requests** toggle to disable this service so passwords can not be requested. NOTE: Disabling the password request service will place any open requests on hold until this service is reenabled.
SSH Key Requests	SSH key requests are enabled by default, indicating that

Setting	Description
	authorized users can make SSH key release requests Click the **SSH Key requests** toggle to disable this service so SSH keys can not be requested. NOTE: Disabling the SSH Key request service will place any open requests on hold until this service is reenabled.
API Key Requests	API key requests are enabled by default, indicating that authorized users can make API key release requests Click the **API Key requests** toggle to disable this service so API keys can not be requested. NOTE: Disabling the API Key request service will place any open requests on hold until this service is reenabled.
Password Management	
Check Password Management	Check password management is enabled by default, indicating that SPP automatically performs the password check task if the profile is scheduled, and allows you to manually check an account's password. Click the **Check password management** toggle to disable the password validation service. NOTE:SPP enables automatic password management services by default. Typically, you would only disable them during an organization-wide maintenance window. When disabling a password management service, SPP allows all currently running tasks to complete; however, no new tasks will be allowed to start.
Change Password Management	Change password management is enabled by default, indicating that SPP automatically performs the password change task if the profile is scheduled, and allows you to manually reset an account's password. Click the **Change password management** toggle to disable the password reset service. NOTE:SPP enables automatic password management services by default. Typically, you would only disable them during an organization-wide maintenance window. When disabling a password management service, SPP allows all currently running tasks to complete; however, no new tasks will be allowed to start.
SSH Key Management	
Check SSH Key	SSH key check is enabled by default, indicating that SSH key

Setting	Description
	check is managed per the profile governing the partition's assigned assets and the assets' accounts. Click the **Check SSH Key** toggle to disable the check service.
Change SSH Key	SSH key change is enabled by default, indicating that SSH key change is managed per the profile governing the partition's assigned assets and the assets' accounts. Click the **Change SSH Key** toggle to disable the change service.
API Key Management	
Check API Key	API key check is enabled by default, indicating that API key check is managed per the profile governing the partition's assigned assets and the assets' accounts. Click the **Check API Key** toggle to disable the check service.
Change API Key	API key change is enabled by default, indicating that API key change is managed per the profile governing the partition's assigned assets and the assets' accounts. Click the **Change API Key** toggle to disable the change service.
Discovery	
Asset Discovery	Asset discovery is enabled by default, indicating that available Asset Discovery jobs find assets by searching directory assets, such as Active Directory, or by scanning network IP ranges. For more information, see Discovery.
Account Discovery	Account discovery is enabled by default, indicating that available Account Discovery jobs find accounts by searching directory assets such as Active Directory or by scanning local account databases on Windows and Unix assets (`/etc/passwd`) that are associated with the account discovery job. For more information, see Discovery.
Service Discovery	Service discovery is enabled by default, indicating that available Service Discovery jobs find Windows services that run as accounts managed by Safeguard. For more information, see Discovery on page 364.
SSH Key Discovery	SSH key discovery is enabled by default. With the toggle on, SSH keys in managed accounts are discovered. For more information, see SSH Key Discovery on page 398.
Directory	
Directory Sync	Directory sync is enabled by default, indicating that additions or deletions to directory assets are synchronized. You can set the number of minutes for synchronization. For more information, see

Setting	Description
	Management tab (add asset).
Audit Log Stream	
Audit Log Stream Service	Use this to send SPP data to Safeguard for Privileged Sessions to audit the Safeguard privileged management software suite. The feature is disabled by default. To accept SPP data, the Safeguard for Privileged Sessions Appliance Administrator must turn on audit log syncing. For information, see the *Safeguard for Privileged Sessions Administration Guide*. SPP and Safeguard for Privileged Sessions must be linked to use this feature. For more information, see SPP and Safeguard for Privileged Sessions appliance link guidance. While the synchronization of SPP and Safeguard for Privileged Sessions is ongoing, Safeguard for Privileged Sessions is not guaranteed to have all of the audit data at any given point due to some latency. NOTE: This setting is also available under **Security Policy Management** > **Settings**. For more information, see Security Policy Settings.
SCIM Provisioning	
SCIM Provisioning	Use this toggle to enable or disable SCIM provisioning on the appliance. For more information, see Adding identity and authentication providers.
Application to Application	
Application to Application	Use this toggle to enable or disable the application to application connection behind a web application firewall via the TLS termination reverse proxy. The following configuration information is displayed and can be updated using the button: • **TLS Termination Reverse Proxy Subnet (CIDR format)**: The subnet for the TLS termination reverse proxy. • **Service Port**: The service port used for connecting. By default this is port 443.

Table 46: Global Services settings

Setting	Description
Disable All	Appliance Administrators can use this button to disable all services (as long as at least one service is currently enabled). A dialog will appear asking for

Setting	Description
	confirmation before disabling the services. You will need to reenable each service individually.

External Integration

The Appliance Administrator can:

- Configure the appliance to send event notifications to various external systems.
- Integrate with an external ticketing system or track generic ticket numbers.
- Configure both external and secondary authentication service providers.

Go to External Integration:

- web client: Navigate to **Appliance Management** > **External Integration**.

Table 47: External Integration settings

Setting	Description
Email	Where you configure SPP to automatically send email notifications when certain events occur.
Email Templates	Where you configure SPP email templates.
Hardware Security Module	Where you configure the Hardware Security Module integration, which allows SPP to utilize an external Hardware Security Module device for encryption.
SNMP	Where you configure SPP to send SNMP traps to your SNMP console when certain events occur.
Starling	Where you join SPP to Starling to take advantage of Starling services.
Syslog	Where you configure SPP to send event notifications to a syslog server with details about the event.
Syslog Events	Where, using an existing syslog server, you create a subscriber and assign events.
Ticket systems	Where you configure SPP to integrate with your company's external ticket system or track generic tickets and not integrate with an external ticketing system.
Trusted Servers, CORS, and Redirects	Where you can restrict login redirects and Cross Origin Resource Sharing (CORS) requests to a specified list of IP addresses, host names (including DNS wildcards), and CIDR notation networks.

Email

It is the responsibility of the Appliance Administrator to configure SPP to automatically send email notifications when certain events occur.

Use the **Email** pane to configure the SMTP server to be used for email notifications and to edit the email templates that define the content of email notifications.

Before you start

Before configuring the SMTP server, perform the following, as needed.

- Configure the DNS Server and set up the user's email address correctly.
- If you are using a transport layer for email authentication, it is recommended you create the certificate signing request (CSR) with SPP using the **Add Certificate** > **Create Certificate Signing Request (CSR)** option. For more information, see Creating an audit log Certificate Signing Request on page 177.

  CSRs may be installed in the following formats.

  - Install Certificate generated from CSR including:
    - DER Encoded Files (.cer, .crt, or .der)
    - PEM Encoded Files (.pem)
  - Install Certificate with Private Key including:
    - PKCS#12 (.p12 or .pfx)
    - Personal Information Exchange Files (.pfx)

To configure the SMTP Server

1. Go to SMTP Server:
   - web client: Navigate to **External Integration** > **Email**.
2. To configure the email notifications, enter these global settings for all emails:
   - **SMTP Server Address**: Enter the IP address or DNS name of the mail server. When unspecified, the email client is disabled.
     When entering an IPv6 address, you must encapsulate it in square brackets, such as `[b86f:b86f:b86f:1:b86f:b86f:b86f:b86f]`.
     If you are using a mail exchanger record (MX record), you must specify the domain name for the mail server.
   - **SMTP Port**: A default port is set for SMTP which should be changed, if needed. By default, the SMTP port is 465 or, if you are using SSL/TLS, the default is port 25. The range is 1 to 65535.
   - Select one of the following to add **Transport Layer Security**.
     - **Require STARTTLS**: Select this option to connect to an SMTP server that supports the STARTTLS command to elevate the connection from text-based to TLS.

- **Require SMTPS**: Select this option to immediately use TLS in its connection to the target SMTP server.
- **None**: There is no transport layer security applied to emails.

If you selected **Require STARTTLS** or **Require SMTPS**, you can select one, both, or none of the following:

- **Verify SSL Certificate**: Verify SSL Certificate: If not selected, the remote SMTP server's SSL certificate is not verified.
- **Use Client Certificate**: Select this check box to present a Client Certificate during a TLS connection to the remote SMTP server.

- **User Authentication**: Select an option if you want to authenticate access to the SMPT server.
  - **Account**: If selected, click **Directory Account** or **Asset Account** then select the account to use for authentication.
  - **Password**: If selected, enter the **Account Name** and **Account Password** to use for authentication.
  - **None**: If selected, the user will not be authenticated.
- **Send Test Email To**: Enter an email address to use as the "From" address for all emails originating from the appliance. This is required if you specify the **SMTP Server Address**. The limit is 512 characters.

To validate your setup

Test the email setup. When you test, no emails except for the tests are handled.

1. In **Send Test Email To**, enter the email address of where to send the test message.
2. Enter the **Timeout** for the test email from delivery start to the email successfully being sent or the return of an error notification. Each IP address is tested and if one fails, the an error is returned for the entire process. The maximum is 255 seconds per IP check. The error logs are maintained for two days. During testing, a valid **From** address with an invalid **To** address is not delivered.
3. Click **Send Test Email**. The email is sent using the configuration settings. If there is an error or timeout, a message displays in the user interface.
4. You must check to ensure the email is delivered. If there was no message in the user interface but the email is not delivered, check the support bundle log files in the `SMTPSVC1` folder. Two days of logs are maintained. For more information, see Support bundle on page 148.

Enabling email notifications

For users to receive email notifications, there are a few things you must configure properly.

To enable email notifications

1. Users must set up their email address correctly.
    a. Local users:
        i. The Authorizer Administrator or User Administrator sets this up in the user's **Contact Information**. For more information, see Adding a user on page 541.

        -OR-

        ii. Users set this up in their **My Account** settings.
    b. Directory users must have their email set in the Active Directory or LDAP domain.
2. The Appliance Administrator must configure the SMTP server. For more information, see Email on page 218.

TIP: You can setup email subscriptions to any email event type through the API: https://<Appliance IP>/service/core/swagger/ui/index#/EventSubscribers. For more information, see Using the API on page 44.

Email Events

The **Email Events** page is used for adding and managing the subscribers that receive emails for specific SPP events.

Go to Email Events:

- web client: Navigate to **External Integration** > **Email Events**.

The **Email Events** pane displays the following about the subscribers defined.

Table 48: Email Events: Properties

Property	Description
Subscriber	The name of the email event recipient.
Description	The description of the email event.
Shared	This column displays a check mark if all Appliance Administrators will see information on the email event subscription on their **Email Events** page.
# of Events	The number of events sent in the email.

Use these toolbar buttons to manage the email event subscribers

Table 49: Email Event: Toolbar

Option	Description
Add	Add a new email event subscriber. For more information, see Add an email event.
Remove	Remove the selected email event from SPP.
Edit	Modify the email event.
Copy	Clone the selected email event.
Show System Owned/ **Hide System Owned**	Use these buttons to either display or hide system owned email events from list.
Refresh	Update the list of email events.
Send Test Event	To send a test message.

Add an email event

It is the responsibility of the Appliance Administrator to add an event.

To add an email event

1. Navigate to **External Integration** > **Email Event**.
2. Click **+ Add** to display the **Email Events Subscription** dialog.
3. In the **Email Events Subscription** dialog, enter the following:
   a. **Email Address**: Enter the email address of the recipient or use the **Browse** button.
   b. **Description**: Enter the description of the event.
   c. **Subscribe to All Events**: Select this check box to subscribe to all events, including new events that may be added in the future. If unselected, select specific events.

      Make sure that the user creating the event has sufficient permission to receive all of the events configured. If the event is configured by a user with inadequate permissions to receive all the events that are configured, some events may not be received. If this happens, delete the email event and recreate it as a user that has sufficient permission.
   d. If you left **Subscribe to All Events** unselected, click **Browse** then select the check boxes of the **Events** to which you want to subscribe You can enter

characters then click **Search** to limit the events that are displayed. Click **OK**.

4. Click **OK**.

Email Templates

SPP provides default email templates for most events, such as **Cluster Primary Quorum Fails** or **Access Request Denied**. Each event type triggers an email notification that uses the template.

Go to Email Templates:

- web client: Navigate to **External Integration** > **Email Templates**.

Use these toolbar buttons to manage email templates.

Table 50: Email template: Toolbar

Property	Description
Reset	Reset the selected template to the default.
Edit	Modify the selected email template.
Refresh	Update the list of email templates.
Search	To locate a specific template, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Macro properties

Each event type supports specific macros in the template that are appropriate for that type of event. When editing a template, you can click **Insert Event Property** to select properties to insert into the text of the **Subject** line or **Body** using keywords surrounded by double braces. For example, you may select the following event properties in the **Subject** of your email:

```
Access Policy Created {{EventDescription}} {{PolicyId}}
```

SPP ignores macros that are not supported by the event type. Unsupported macros appear blank in the email preview. Additionally, a warning message like the following may displays: `Invalid format for BodyTemplate property.`

To edit an email template

Modify an email template to change any information except the **Event** type. If you later want to revert to the original template, you can select the template then click **Reset** . To modify an email template, use the following steps.

1. Go to Email Templates:
   - web client: Navigate to **External Integration** > **Email Templates**.
2. In the **Email Template** grid, select the template to modify and click. **Edit**.
   a. **Event**: For more information, see Enabling email notifications on page 219.
   b. **Subject**: Edit the subject line for the email message.

      As you type, click **+ Insert Event Property Macro** to insert predefined text into the subject line. For example, you may create the following subject line:

      ```
      Approval is required for {{Requester}}'s request
      ```

      where SPP generates the data defined by the macro within the double braces.

      Limit: 1024 characters
   c. **Reply to**: Enter the email address of the person to reply to concerning this notification.

      Limit: 512 characters
   d. **Body**: Enter the body of the message.

      As you type, click **+ Insert Event Property Macro** to insert predefined text into the body. For example, you may create the following body for an email template:

      ```
      {{Requester}} has requested the password for {{AccountName}} on
      {{AssetName}}
      ```

      where SPP generates the data defined by the macro within the double braces.

      Limit: 16384 characters
   e. **Preview Email**: Select this link to display the **Preview Email** dialog so you can see how your email message will look.
   f. Click **OK**. The updated template is added to the Email Template grid.
3. If you want to return to the default, select the email template then click **Reset**.

Hardware Security Module

It is the responsibility of the Appliance Administrator to configure Safeguard for Privileged Passwords to integrate with an external Hardware Security Module for encryption.

Use the Hardware Security Module pane to configure the Hardware Security Module integration. The following Hardware Security Modules are supported:

- Thales Luna 7.X
- Thales Luna 6.X
- Thales Data Protection on Demand

Go to Hardware Security Module:

- web client: Navigate to **Appliance Management** > **External Integration** > **Hardware Security Module**.

Before you start

Before configuring the Hardware Security Module integration, the Thales Luna environment needs to be fully installed and configured. This includes but is not limited to:

- Setting the Crypto Officer password.
- Generating the Hardware Security Module server certificate(s) (network Luna only).
- Generating a Hardware Security Module client certificate for each Safeguard for Privileged Password clustered appliance (network Luna only).
- Initializing a partition.
- Creating any high availability groups Safeguard for Privileged Passwords will utilize.

SPP will require the following information to configure the integration:

- Crypto Officer password
- Server certificate(s) (network Luna only)
- Client certificate(s) (network Luna only)
- Partition label (can be high availability group label)
- crystoki.ini file

If you are configuring an integration that includes a network Luna device, first install and assign the Hardware Security Module client and server certificates for your environment. For more information, see Installing a Hardware Security Module client certificate, Assigning a Hardware Security Module client certificate, and Uploading a Hardware Security Module server certificate.

IMPORTANT: Connection to network Luna devices is only supported through a Network Trust Links (NTLs) connection. Secure Trusted Channel (STC) connections are not supported when integrating with SPP.

CAUTION: It is best practice to only enable or disable a Hardware Security Module integration on a standalone SPP appliance. The encrypted data stored within the SPP appliance will be re-encrypted during these operations. If enabling or disabling in a clustered environment, the cluster will be broken and the primary SPP appliance will be set to a standalone appliance and all replica's will need to be rejoined to the cluster after the maintenance task has been completed. During this time ensure that no operations that use encrypted data, such as password check and change are performed on the replica appliances to avoid data corruption.

CAUTION: SPP will use a reserved label for the encryption key stored on the Hardware Security Module partition. These labels cannot exist on the partition when doing an integration for the first time. The reserved key label name is:

`SafeguardMasterKey1`

CAUTION: When configuring an integration that includes network Luna devices, ensure all client and server certificates have been installed on the primary SPP appliance for all future cluster members. In addition, install and assign the required client certificates on the replicas prior to joining the cluster.

To configure the Hardware Security Module integration

1. Go to Hardware Security Module:
   - web client: Navigate to **Appliance Management** > **External Integration** > **Hardware Security Module**.
2. Select the **Use External HSM** checkbox.
3. In the **Partition Label** field, enter the partitional label SPP should use on the Hardware Security Module device.
4. Enter the Crypto Officer password SPP should use to connect to the Hardware Security Module device.
5. Click **Upload File** and browse for the crystoki.ini configuration file.
6. Once selected, click **Open**.
7. Click **Save**.

   NOTE: If there is an error with SPP ability to move forward with the integration based on the provided configuration, a message displays in the user interface with further information.

Once you have finished configuring the Hardware Security Module integration, the following information and options will be available:

Table 51: Hardware Security Module: Properties

Setting	Description
Health Status	Displays the results of the last Hardware Security Module verification.
Refresh	Runs a Hardware Security Module verification. This can be used to transition a SPP appliance out of the HardwareSecurityModuleError state.
Last Successful Access Date	The date and time of the last **Healthy** Hardware Security Module status.
Show Details	Shows the current crystoki.ini contents being used for the Hardware Security Module integration.

To disable the Hardware Security Module integration

1. Go to Hardware Security Module:
   - web client: Navigate to **Appliance Management** > **External Integration** > **Hardware Security Module**.
2. Deselect the **Use External HSM** checkbox.
3. Click **Save**.

SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. One Identity Safeguard for Privileged Passwords allows you to configure SNMP subscriptions for sending SNMP traps to your SNMP console when certain events occur.

Go to SNMP:

- web client: Navigate to **External Integration** > **SNMP**.

The **SNMP** pane displays the following about the SNMP subscribers defined.

Table 52: SNMP: Properties

Property	Description
Network Address	The IP address or FQDN of the primary SNMP network server.
Port	The UDP port number for SNMP traps.
Version	The SNMP version being used.
Description	The description of the SNMP subscriber.
Community	The SNMP community string being used by the SNMP subscriber.
Authentication Type	The type of authentication.
Encryption Type	The type of encryption.
# of Events	The number of events selected to be sent to the SNMP console.

Use these toolbar buttons to manage the SNMP subscriptions.

Table 53: SNMP: Toolbar

Option	Description
+ **Add**	Add a new SNMP subscription. For more information, see Configuring SNMP subscriptions on page 227.

Option	Description
Remove	Remove the selected SNMP subscription.
Edit	Modify the selected SNMP subscription.
Copy SNMP Template	Clone the selected SNMP subscription.
Refresh	Update the list of SNMP subscriptions.

Configuring SNMP subscriptions

It is the responsibility of the Appliance Administrator to configure SPP to send SNMP traps to your SNMP console when certain events occur.

You can create a test to verify the SNMP configuration. For more information, see Verifying SNMP configuration on page 228.

To download SPP MIB-module definitions from your appliance, enter the following URL into your web browser; no authentication is required:

```
https://<Appliance IP address>/docs/mib/SAFEGUARD-MIB.mib
```

To configure SNMP subscriptions

1. Go to SNMP:
   - web client: Navigate to **External Integration** > **SNMP**.
2. Click **+ Add** to open the **SNMP subscription configuration** dialog.
3. Provide the following information:
   - **Network Address**: Enter the IP address or FQDN of the primary SNMP network server. Limit: 255 characters
   - **UDP Port**: Enter the UDP port number for SNMP traps. Default: 162
   - **Description**: Enter the description of the SNMP subscriber. Limit: 255 characters
   - **Subscribe to All Events**: Select this check box to subscribe to all events.
   - **Events**: Available when **Subscribe to All Events** is not selected, click **Browse** to select one or more SNMP event types. Use the **Clear** icon to remove an individual event from this list and select **Remove All** to clear all events from the list. The **SNMP** pane displays the number of events that you select, not the names of the events.
   - **Version**: Choose the SNMP version. Default: Version 2c. Depending on the version selected, the following fields appear:

- Version 1 and Version 2c:
  - **Community**: Enter the SNMP community string, such as public. The SNMP community string is like a user ID, password that allows access to a device's statistics, such as a router. A PRTG Network Monitor sends the community string along with all SNMP requests. If the community string is correct, the device responds with the requested information. If the community string is incorrect, the device simply discards the request and does not respond.
- Version 3:
  a. **Engine ID**: Enter the Engine ID that is used as a unique identifier for SNMPv3 entities.
  b. **Authentication User Name**: Enter the user name that will be used to establish a connection.
  c. **Authentication Type**: Select the type of authentication to use: **None** (if selected there is no additional configuration required), **MD5**, or **SHA1**.
  d. **Authentication Password**: Enter the password associated with the user entered in the **Authentication User Name** field.
  e. **Encryption Type**: Select the type of encryption: **None** (if selected there is no additional configuration required), **DES**, **AES128**, **AES192**, **AES256**, or **TripleDES**.
  f. **Encryption Password**: Enter the password associated with the selected **Encryption Type**.

4. Click **OK**.

Verifying SNMP configuration

Use the **Send Test Event** link located under the SNMP table to send a test event to verify the SNMP configurations.

To validate your setup

1. Go to SNMP:
   - web client: Navigate to **External Integration** > **SNMP**.
2. When configuring your SNMP subscription, on the **SNMP** dialog, add the test event to your event subscription. For more information, see Configuring SNMP subscriptions on page 227.
3. On the **SNMP** settings pane:
   a. Select the SNMP configuration from the table.
   b. Click **Send Test Event**. SPP sends a test event notification to your SNMP console.

Starling

SPP can join with the cloud platform One Identity Starling. By joining with One Identity Starling, SPP customers can take advantage of companion features from multiple Starling services. In addition, once SPP has joined with Starling, a Starling Identity and Authentication provider will automatically be added to Safeguard. However, there won't be any users or groups available until an administrator adds a Microsoft Azure Active Directory tenant to their Starling organization via the **Directories** settings page in Starling. For more information, see the following sections:

- Join Starling
- After joining Starling
- Unjoin Starling

Join Starling

In order to use the SPP features associated with Starling services, you must join SPP to Starling. It is the responsibility of the Appliance Administrator to join One Identity Safeguard for Privileged Passwords to Starling.

For additional information and documentation regarding the Starling Cloud platform and services, see the One Identity Documentation.

Prerequisites

See the Starling Release Notes for currently supported platforms.

In order to use the companion features from Starling services, first configure the following:

- Register a Starling organization. For more information on Starling, see the One Identity Starling User Guide.

  > IMPORTANT: Not all Starling services are available to organizations in both the United States and European Union data centers. Check the documentation for the Starling services to see if there are any data center restrictions.

- If your company requires the use of a proxy to access the internet, you must configure the web proxy to be used. For more information on configuring a web proxy to be used by SPP for outbound web requests to integrated services, see Networking.
- To use the Cloud Assistant feature, you must subscribe to the Starling Cloud Assistant feature and configure the channel(s) that will be used.

Join SPP with Starling

> NOTE: You must be an Organization Admin for the Starling organization in order to join SPP with Starling.

1. Go to Starling:
   - web client: Navigate to **External Integration** > **Starling**.
2. Notice that this pane also includes the following links, which provide assistance with Starling:
   - **Visit us online to learn more** displays the Starling login page where you can create a new Starling account.
   - **Trouble Joining** displays the Starling support page with information on the requirements and process for joining with Starling.
3. Click **Join to Starling** and follow the prompts to complete the process.
   The following additional information may be required:
   - If you do not have an existing session with Starling, you will be prompted to authenticate.
   - If your Starling account belongs to multiple organizations, you will be prompted to select which organization SPP will be joined with.
4. After the join has successfully completed, you will be returned to the SPP client and the **Starling** pane will now show **Joined to Starling**. For information on the features that are now available, see After joining Starling. For information on unjoining from Starling, see Unjoin Starling.

   > IMPORTANT: In order to use the Cloud Assistant feature, once you have joined with Starling you must enable the **Register as a sender with Cloud Assistant** toggle on the **External Integration** > **Starling** pane.

After joining Starling

Once SPP is joined to Starling, the following SPP features are enabled:

Feature using Starling Connect

- Starling Connect Registered Connectors

  This feature integrates your Starling connectors with SPP. This allows for the accounts stored in the connectors to be discovered and controlled by SPP through the use of partitions which allow for rotating passwords to provide additional security for them. For more information, see Registered Connectors

Feature using Starling Cloud Assistant

- Cloud Assistant

  The Cloud Assistant feature integrates its access request workflow with Starling Cloud Assistant, allowing approvers to receive a notification through a configured channel when an access request is submitted. The approver can then approve (or

deny) access requests through the channel without needing access to the SPP web application.

The Cloud Assistant feature is enabled when you join SPP to Starling. For more information, see Starling on page 229. Once enabled, it is the responsibility of the Security Policy Administrator to define the users who are authorized to use Cloud Assistant to approve access requests.

> IMPORTANT: In order to use the Cloud Assistant feature, once you have joined with Starling you must enable the **Register as a sender with Cloud Assistant** toggle on the **External Integration** > **Starling** pane.

Feature using Connect for Safeguard Assets

- Connect for Safeguard Assets

  Within Starling, a Connect for Safeguard Assets service is available. Once added, this service allows for assets not connected to your corporate network to use the check and change passwords functionality of SPP. For more information, see the *Connect for Safeguard Assets User Guide* available as part of the SPP documentation.

  > IMPORTANT: Regardless of the version of SPP you are using, the *Connect for Safeguard Assets User Guide* associated with the latest version of SPP should always be used when configuring a new agent. This is available from the SPP documentation site.

Starling as an identity provider

Once SPP has joined with Starling, a Starling Identity and Authentication provider will automatically be added to Safeguard. This is indicated by the **Realm(s)** section under **Starling**. However, there won't be any users or groups available until an administrator adds a Microsoft Azure Active Directory tenant to their Starling organization via the **Directories** settings page in Starling.

Using Starling as an identity provider

1. Join SPP with Starling. For more information, see Join Starling.
2. Enable a Microsoft Azure Active Directory tenant in your Starling organization (multiple Microsoft Azure Active Directory tenants can be added to Starling, but they will be available and treated as a single tenant when used by Safeguard). This is done via the **Directories** settings page in Starling. For more information, see the Starling User Guide.
3. In order for Safeguard users to authenticate against Starling, a Relying Party Trust Application must be created in Starling via the **Applications** settings page. For more information, see the Starling User Guide.

   To create the application in Starling, you will need to **Download Safeguard Federation Metadata** from Identity and Authentication

   > NOTE: You cannot use the Add OpenID Connect Application with SPP.

4. You will need to enter one or more values in the **Realm(s)** section to associate with the new Starling authentication provider. This will then allow users logging in to Safeguard to select External Federation and use Starling for their authentication.
5. When the **Require User to Always Authenticate** check box is selected, the user will always be required to enter their credentials on the external provider, regardless of whether they are already logged in.

Adding new users and groups to Safeguard that come from Starling follows the same process as with other directory based identity providers (such as, Active Directory and LDAP) and the user information will be periodically synchronized from Starling.

> IMPORTANT: You may need to restart the client in order for Starling to appear as an available identity provider.

Unjoin Starling

It is the responsibility of the Appliance Administrator to unjoin One Identity Safeguard for Privileged Passwords from Starling.

For additional information and documentation regarding the Starling Cloud platform and services, see the One Identity Documentation.

To unjoin SPP from Starling

1. Go to Starling:
   - web client: Navigate to **External Integration** > **Starling**.
2. Click **Unjoin Starling**.

   > IMPORTANT: If there is an issue with the connection to Starling, a warning message will appear on the page and you will instead see a **Force Unjoin** button.
3. SPP will no longer be joined to Starling, which means that Cloud Assistant, Starling identity providers, and integrated connectors are also disabled in SPP. A Starling Organization Admin account can rejoin SPP to Starling at any time.

   > IMPORTANT: If you attempt to unjoin from Starling while there are still Safeguard users or groups that use the Starling provider for identity and authentication, you will get an error. You must manually delete any users or groups first before unjoining from Starling.

Syslog

SPP allows you to define one or more syslog servers to be used for logging SPP event messages. Appliance Administrators can specify to send different types of messages to different syslog servers. You may configure a connection to a syslog server to use TLS encryption, with or without a client authentication certificate. For more information, see Syslog Client Certificate on page 190.

To define and manage the syslog servers, go to Syslog:

- web client: Navigate to **External Integration** > **Syslog**.

The **Syslog** pane displays the following about each syslog server defined.

Table 54: Syslog server: Properties

Property	Description
Name	The name of the syslog server
Network Address	The IP address or FQDN of the syslog server
Port	The port number for syslog server
Protocol	The network protocols and syslog header type
TCP Framing	When using syslog with the TCP protocol, since the connection is stream based both the client and server need to be configured to process the data using the same delimiter. See RFC 6587 section 3.4.1 and 3.4.2 for more details. By default, SPP will use octet counting, as is recommended by RFC 6587. However, some syslog servers do not support octet counting. If that is the case, use this setting to configure SPP to use the delimiter that is supported by your syslog server.
Use TLS Encryption	If ✔ selected, provides encrypted communication with the syslog server instead of plain text over TCP
Use Client Certificate	If ✔ selected, the syslog server requires clients to authenticate
Verify Server Certificate	If ✔ selected, the syslog server certificate messages will only be sent if SPP is able to verify the authenticity of the syslog server TLS certificate

Use these toolbar buttons to manage the syslog server configurations

Table 55: Syslog server: Toolbar

Option	Description
Add	Add a new syslog server configuration. For more information, see Configuring and verifying a syslog server on page 234.
Remove	Remove the selected syslog server configuration from SPP. If you attempt to remove a syslog server in use, you will see a message like: `<syslog server> will be removed`. Select **Yes** or **No**. A second `Force Delete` message like this may display: `There are dependencies on this syslog server: This object is referenced by ServiceDebug. Do you want to force delete`

Option	Description
	`this server?` Select **Force Delete** or **Cancel**. If you select **Force Delete**, the dependent setting (such as an event subscriber or debug logging) will be deleted as well.
Edit	Modify the selected syslog server configuration.
Copy Syslog Template	Clone the selected syslog server configuration.
Refresh	Update the list of syslog server configurations.

Configuring and verifying a syslog server

It is the responsibility of the Appliance Administrator to configure SPP to log event messages to a syslog server. The steps below cover configuration.

Other considerations:

- For event messages to be logged, you must configure SPP to send alerts. For more information, see Configuring alerts on page 95.
- The syslog client certificate will be used. For more information, see Syslog Client Certificate on page 190.

To configure a syslog server

1. Go to Syslog:
   - web client: Navigate to **External Integration** > **Syslog**.
2. Click **+ Add** to display the **Syslog Server**dialog.
3. In the **Syslog Server** dialog, enter the following:
   a. **Name**: Enter a descriptive name for the syslog server.
   b. **Network Address**: Enter the IP address or FQDN of the syslog server. Limit: 255 characters
   c. **Port**: Enter the port number for the syslog server. Default: 514 and range: between 1 and 32767
   d. **Protocol**: Select the network protocol and syslog header type:
      - UDP (RFC 3164): Sends messages over UDP using the syslog header format specified in RFC 3164.
      - UDP (RFC 5424): Sends messages over UDP using the syslog header format specified in RFC 5424.
      - TCP (RCF 5424): Sends messages over TCP using the syslog header format specified in RFC 5424. TCP is required for TLS options.

e. If you selected a **Protocol** of **TCP (RCF 5424)**, additional selections can be made to set the TCP framing and configure SPP to use Transport Layer Security (TLS). This provides encrypted communication with the syslog server instead of plain text over TCP.

- Select the **TCP Framing**. By default, **Octet Counting** will be selected. Possible options are:
  - **Octet Counting**: The default and recommended framing. For more information, see https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.1. With octet counting, there is no chance of a message containing a character that may otherwise be intended to be used as a delimiter.
  - **LF**: Use a line feed character (LF 0x0A) as the delimiter between syslog messages. For more information, see https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2. Note that the RFC describes problems with using this framing and is therefore not recommended. However, some syslog servers do not support octet counting and must use one of these non-transparent framing options. Safeguard for Privileged Passwords makes no attempt to escape out this character if it appears in a message itself. If that happens, you will receive a fragmented and potentially malformed message/data.
  - **CR**: Use a carriage return character (CR 0x0D) as the delimiter between syslog messages. For more information, see https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2. Note that the RFC describes problems with using this framing and is therefore not recommended. However, some syslog servers do not support octet counting and must use one of these non-transparent framing options. Safeguard for Privileged Passwords makes no attempt to escape out this character if it appears in a message itself. If that happens, you will receive a fragmented and potentially malformed message/data.
  - **CRLF**: Use both carriage return and line feed characters (CRLF 0x0D0A) as the delimiter between syslog messages. For more information, see https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2. Note that the RFC describes problems with using this framing and is therefore not recommended. However, some syslog servers do not support octet counting and must use one of these non-transparent framing options. Safeguard for Privileged Passwords makes no attempt to escape out this character if it appears in a message itself. If that happens, you will receive a fragmented and potentially malformed message/data.

- **NUL**: Use a NUL character (0x00) as the delimiter between syslog messages. For more information, see https://datatracker.ietf.org/doc/html/rfc6587#section-3.4.2. Note that the RFC describes problems with using this framing and is therefore not recommended. However, some syslog servers do not support octet counting and must use one of these non-transparent framing options. Safeguard for Privileged Passwords makes no attempt to escape out this character if it appears in a message itself. If that happens, you will receive a fragmented and potentially malformed message/data.

- Select **Use TLS Encrypton**.
- **Verify Syslog Server Certificate**: If selected, the syslog server certificate messages will only be sent if SPP is able to verify the authenticity of the syslog server TLS certificate. If SPP cannot resolve the syslog server TLS certificate to a trusted root, the message will not be sent.
- **Use Client Certificate**: Select this option if the syslog server requires clients to authenticate. You should also set the syslog client certificate appropriately. For more information, see Creating a syslog client Certificate Signing Request on page 192.

4. Click **OK** to save your selection and add the syslog server configuration.
5. You can verify the syslog server. See the next section.

To verify a syslog server

1. Navigate to ⇌ **External Integration** > **Syslog Event**.
2. Click **Send Test Event**. For more information, see Syslog Events on page 236.

Syslog Events

You can configure audit event logs to send to syslog server (cluster-wide). Audit events include connection, closure, and failures. Failures include the reason, the initiator, and the target. For example, a certificate validation failure will include the initiator and the target.

Debug logging to syslog server is available and is appliance specific (see Debug).

To configure audit event logs to send to a syslog server

1. You will need a configured syslog server. If you have not configured a syslog server, you will see a message like this: `To configure additional debut logging options, you need to configure a syslog server.` Click **Configure a syslog server**. For more information, see Configuring and verifying a syslog server on page 234.
2. Navigate to ⇌ **External Integration** > **Syslog Events**.
3. The **Syslog Events** pane displays the following.

Table 56: Syslog server: Properties

Property	Description
Syslog Server	The name of the syslog server
Facility	The type of program being used to create syslog messages (for example, User or Mail)
Log Format	The format which can be CEF or JSON
Description	The description of the syslog event
# of Events	The number of events selected to be logged to the syslog server

Use these toolbar buttons to manage the syslog server configurations

Table 57: Syslog server: Toolbar

Option	Description
Add	Add a new syslog server configuration. For more information, see Configuring and verifying a syslog server on page 234.
Remove	Remove the selected syslog server configuration from SPP.
Edit	Modify the selected syslog server configuration.
Copy Syslog Template	Clone the selected syslog server configuration.
Refresh	Update the list of syslog server configurations.
Send Test Event	To send a test message to the designated syslog server

Add a syslog event subscriber

It is the responsibility of the Appliance Administrator to add an event subscriber.

To add an event subscriber

1. Navigate to **External Integration** > **Syslog Event**.
2. Click **Add** to display the **Syslog Events** dialog.
3. In the **Syslog Events** dialog, enter the following:
   a. **Syslog Server**: Select the server to which you want to send the events.
   b. **Description**: Enter the description of the syslog event.

c. **Subscribe to All Events**: Select this check box to subscribe to all events, including new events that may be added in the future. If unselected, select specific events.

   Make sure that the user creating the Syslog Event entry has sufficient permission to receive all of the events configured. If the Syslog Event entry is configured by a user with inadequate permissions to receive all the events that are configured, some events may not be received. If this happens, delete the Syslog Event entry and recreate it as a user that has sufficient permission.

d. If you left **Subscribe to All Events** unselected, click **Browse** then select the check boxes of the **Events** to which you want to subscribe You can enter characters then click **Search** to limit the events that are displayed. Click **OK**.

e. **Facility**: Select which syslog facility to send, for example User or Mail.

f. **Log Format**: Select between Common Event Format (CEF) or Javascript Object Notation (JSON).

g. If you select JSON, enter the **Attribute Prefix** which is text that will be prepended to the JSON attributes.

4. Click **OK**.

Ticket systems

You can use ticketing that is not configured with an external ticketing system or integrate with an external ticketing system (such as ServiceNow or Remedy).

Tickets can be viewed in the Activity Center, **Ticket #** column.

Go to Ticket Systems:

- web client: Navigate to **External Integration** > **Ticket Systems**.

Ticketing toolbar

Use these toolbar buttons to manage the ticketing systems defined to integrate with SPP.

- **Add**: Add a new ticket system.
- **Remove**: Remove the selected ticket system from SPP.
- **Edit**: Modify the selected ticket system configuration.
- **Refresh**: Update the list of ticket systems.

Setup and workflow

For set up and workflow details, see the following based on the ticketing you use:

- ServiceNow ticketing system integration
- Remedy ticketing system integration
- Not integrated with ticketing system

ServiceNow ticketing system integration

ServiceNow is a cloud-based issue tracking system. SPP can exchange the following ticket types with ServiceNow:

- INC (incident) tickets
- CHG (change) tickets
- RITM (request) tickets
- PRB (problem) tickets

The data items specific to ServiceNow may be optional based on your configuration.

To use ServiceNow, the root CA Certificate required for ServiceNow must be installed in SPP. For more information, see Trusted CA Certificates on page 193. To add a trusted certificate, see Adding a trusted certificate.

Tickets can be viewed in the Activity Center, **Ticket #** column.

Setting up the integration

1. Go to Ticket Systems:
   - web client: Navigate to **External Integration** > **Ticket Systems**.
2. Click **Add** to add a ticket system.
3. Do the following:
   - web client: Select **ServiceNow**.
4. Complete the authorization information based on your installation:
   - **Name**: Enter the name of your ticketing system
   - **URL**: Enter the web site address to the ticketing system.
   - **Username**: Enter an account for SPP to use to access the ticketing system.
   - **Password**: Enter the user account's password.
   - **Client Identifier**: Enter the ServiceNow Client ID.
   - **Client Secret**: Enter the ServiceNow secret key.
5. Click **Test Connection** to test the connection to ServiceNow.

Ticket workflow

1. The Security Policy Administrator creates an access request policy that requires the requester to provide a ticket number when creating an access request.
2. When the requester makes a request, they must enter the existing ServiceNow ticket number on the **New Access Request** dialog, **Request Details** tab, **Ticket Number** field. See:
   - Requesting a password release
   - Requesting an SSH key release
   - Requesting session access
3. SPP queries all configured ticket systems to see if that ticket number represents a ticket that exists and is in an open state. For ServiceNow, Safeguard checks the Active property of the identified ticket returned from the ServiceNow API and considers the ticket number valid if the Active property is not false for that incident.
   a. If the ticket is not active, the request is denied.
   b. If the ticket is active, the access workflow continues.

Remedy ticketing system integration

You can use ticketing that is configured to work with Remedy.

Tickets can be viewed in the Activity Center, **Ticket #** column.

Safeguard checks the Status property of the incident returned from the Remedy API. The ticket is considered valid if Status is not Closed or Cancelled.

The data items specific to Remedy may be optional based on your configuration.

Setting up the integration

1. Go to Ticket Systems:
   - web client: Navigate to **External Integration** > **Ticket Systems**.
2. Click **Add** to add a ticket system.
3. Do the following:
   - web client: Select **Remedy**.
4. Complete the authorization information based on your installation:
   - **Name**: Enter the name of your ticketing system.
   - **URL**: Enter the web site address to the ticketing system.
   - **Username**: Enter an account for SPP to use to access the ticketing system.
   - **Password**: Enter the user account's password.

- **Authentication String**: Enter the authentication credential for the Remedy AR (Action Request) system server.

5. Click **Test Connection** verify the connection to Remedy works.

Ticket workflow

1. The Security Policy Administrator creates an access request policy that requires the requester to provide a ticket number when creating an access request.
2. When the requester makes a request, they must enter the existing Remedy ticket number on the **New Access Request** dialog, **Request Details** tab, **Ticket Number** field. See:
   - Requesting a password release
   - Requesting an SSH key release
   - Requesting session access
3. SPP queries all configured ticket systems to see if that ticket number represents a ticket that exists and is in an open state.

Not integrated with ticketing system

You can use ticketing that is not configured with an external ticketing system to track tickets.

Tickets can be viewed in the Activity Center, **Ticket #** column.

Security Policy Administrators can require requesters to reference a ticket number in their password, SSH key, or session access request but not have the ticket validated against an external ticketing system but, optionally, may be validated against the regular expression of a generic ticketing system. The ticket number is used in the decision to approve the request.

Setting up ticketing

1. Go to Ticket Systems:
   - web client: Navigate to **External Integration** > **Ticket Systems**.
2. Click **Add** to add a ticket system.
3. Select **Other** and complete this information:
   - **Name**: Enter a name to be used in tracking tickets.
   - **Regular Expression**: Enter the regular expression pattern to validate for an exact match. For more information, see Regular expressions on page 688.
4. Click **Validate** to validate the **Regular Expression** entry.

Ticket workflow

1. The Security Policy Administrator creates an access request policy that requires the requester to provide a ticket number when creating an access request.
2. When the requester makes a request, they must enter a ticket number on the **New Access Request** dialog, **Request Details** tab, **Ticket Number** field. See:
   - Requesting a password release
   - Requesting an SSH key release
   - Requesting session access
3. Safeguard for Privileged Passwords validates the ticket number against the regular expression. If the ticket number is an exact match to the regular expression, the workflow continues.

Trusted Servers, CORS, and Redirects

You can restrict login redirects and Cross Origin Resource Sharing (CORS) requests to a specified list of IP addresses, host names (including DNS wildcards), and CIDR notation networks. By default, a single asterisk (*) means there are no restrictions. This will allow you to easily join multiple Safeguard for Privileged Passwords appliances together to form a cluster. In addition, you will also be able to link to a Safeguard for Privileged Sessions appliance. However, as a best practice, you should change or delete this value after configuring your cluster. It is recommended to set it to the empty string to prevent external CORS requests and login redirects to unknown servers. Or, set it to a list of known servers that integrate with the Safeguard API.

One or more values can be separated by a space, comma, or new line. Do not include the scheme, port, or path. The maximum length for the setting is 512 characters, including separators. Example values and additional details can be seen in the following table.

Table 58: Value detail

IPv4 No reverse DNS lookup will be performed. No scheme or port values are considered.	`10.5.33.37` `192.168.0.2`

IPv6
No reverse DNS lookup will be performed. No scheme or port values are considered.
	`2001:0db8:85a3:0000:0000:8a2e:0370:7334`
	`2001:0db8:85a3:0:0:8a2e:0370:7334`
	`2001:db8::1:0:0:1`
	`2001:db8::2:1`
	`2001:db8::1`

DNS/Host Names Case insensitive match. No scheme or port values are considered. If using	`spp.contoso.corp` `primary.spp.contoso.corp`

Internationalized Domain Names (IDN), you must also manually include the punycode equivalent.	`widget.contoso.corp` `widget`
DNS Wildcards Only one level to the wildcard is allowed, just like SSL certificates. No scheme or port values are considered. If using Internationalized Domain Names (IDN), you must also manually include the punycode equivalent.	`*.spp.contoso.corp` `*.contoso.corp`

CIDR Notation
Any DNS or host name values being validated will have DNS lookup performed to see if any resolved IP addresses are contained within any of the specified CIDR networks. No scheme or port values are considered.
	`10.0.0.0/8`
	`172.16.0.0/12`
	`192.168.0.0/16`
	`76.240.155.0/24`
	`fd12:3456:789a:1::/64`
	`fd00::/8`

Allow All A single asterisk, no other values allowed.	`*`
Allow None Delete all values and leave as the empty string.	

Considerations:

- When adding a new node to the SPP cluster, the node's host name or IP address must be specified in this list, or enter a single asterisk to allow all.
- When linking Safeguard for Privileged Sessions to SPP, the host name or IP address of the Safeguard for Privileged Sessions appliance must be specified in this list, or enter a single asterisk to allow all.
- As a best practice, after clustering (or if using just a single appliance/VM), change the setting value to the empty string or a list of integration applications you wish to allow.

To set up Trusted Servers, CORS and Redirects:

1. Go to Trusted Servers, CORS and Redirects:
   - web client: Navigate to **External Integration** > **Trusted Servers, CORS and Redirects**.
2. **Refresh**: Update the information displayed.
3. In **Allow Hosts**, enter the list of IP addresses, host names (including DNS wildcards), and CIDR notation networks. As mentioned above, the default is a single

asterisk (*) which means there are no restrictions.

4. Click **Save** (web client).

Real-Time Reports

One Identity Safeguard for Privileged Passwords allows you to view real-time information regarding your cluster, appliance schedules, scheduled platform tasks, and appliance resources.

Navigate to **Real-Time Reports** to see the information and options listed below.

Table 59: Real-Time Reports pages

Page	Description
Cluster Information	
Summary	Lists your configured appliances.
<appliance name>	Individual tabs showing information for each appliance.
Session Appliances	Displays the link connections when a Safeguard for Privileged Sessions cluster is linked to a Safeguard for Privileged Password for session recording and auditing.
Appliance Schedules	
Audit Log	Displays information regarding the audit log schedule.
Backup	Displays information regarding the backup schedule for the appliance you are currently logged in to.
Profile Schedule	Displays information regarding the schedules for each profile and discovery type.
Scheduled Platform Tasks	
Appliances	Displays information on the scheduled tasks for each appliance.
Task counts	The left pane displays the individual tasks. Selecting the check box for a task will update the calendar (displayed in the right pane) to show the selected tasks. The right pane displays an interactive calendar view of the tasks. Clicking on a task in the calendar will display additional information regarding the task(s). The following options can be used to navigate the calendar: • : Navigates to today's date. To locate other dates on the calendar, use the following navigation options: , , , ,

Page	Description
	, and . To jump between dates that have tasks associated with them, use the following navigation options: , , , and .
	Views • : Switches to monthly view. • : Switches to weekly view. • : Switches to daily view.
Appliance Resources	
This page displays graphical representations of the resources in use by the appliance you are currently logged in to. Mousing over a graph will provide additional information on the percentages displayed.	

Safeguard Access

SPPallows you to configure settings related to accessing One Identity Safeguard for Privileged Passwords.

Go to Access settings:

- web client: Navigate to **Safeguard Access**.

Table 60: SPP Access settings

Setting	Description
Messaging settings	Where you set Login Notification and the Message of the Day
Local Login Control	Where you configure the user login control settings
Local Password Rule	Where you configure user password complexity rules
Time Zone	Where you can set the time zone and select whether or not users can change their time zone
Identity and Authentication	Where you configure the identity providers and authentication providers to use when logging into SPP

Messaging settings

SPPallows you to set the following notifications.

- web client: Navigate to **Safeguard Access**.

Table 61: Messaging settings

Setting	Description
Login Notification	Where you enable a login banner that users must acknowledge before they can access SPP. This message text can be viewed anonymously.
Message of the Day	Where you set the **Message of the Day** that displays on the Home page page. This is only visible to authenticated users after they have logged in.

Login Notification

It is the responsibility of the Appliance Administrator to configure the login notification displayed when a user logs into One Identity Safeguard for Privileged Passwords. This feature is typically used for describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. Note that the message text can be viewed anonymously. Therefore, you should not include any sensitive information that you don't want read by an unauthenticated user. See the Message of the Day for messages that are only available to authenticated users.

To configure the login notification

1. Go to Messaging:
   - web client: Navigate to **Safeguard Access** > **Messaging**.
2. Type in the **Login Notification** (character limit of 5000).
3. Click **Save**.

Message of the Day

It is primarily the responsibility of the Appliance Administrator to configure the message of the day displayed on the Home page page, however any user with administrator permissions has the ability to set the message of the day. The message is only visible to authenticated users after they have logged in.

To configure the message of the day

NOTE: If you choose RSS, the feed should be HTTPS. The RSS server needs CORS policy enabled.

1. To change the message of the day:
   - web client: Navigate to **Safeguard Access** > **Messaging**.

2. Under **Message of the Day**, choose either the **RSS** or **Subject Line** option.
3. When the **RSS** option is selected, enter a web address of up to 512 characters.
4. When the **Subject line** option is selected, enter the following information:
    - **Subject**: Enter a short description of up to 512 characters.
    - **Message**: Enter message text of up to 512 characters.
5. Click **Save**.

Local Login Control

It is the responsibility of the Appliance Administrator to initially set up user login controls such as the number of failed sign-in attempts before locking out an account.

To configure the login controls

1. Go to Local Login Control:
    - web client: Navigate to **Safeguard Access** > **Local Login Control**.
2. Provide the following information. Some settings are for local users only, such as Lockout Window. Other settings are for all user types, such as the Token Lifetime.

Token Lifetime	Set the number of minutes a user can stay logged into SPP. Range: 10 minutes to 28,800 minutes (20 days) Default: 1,440 minutes (one day)
Web Client Inactivity Timeout	Set the maximum time to allow from the user's last request to the server before the user is automatically logged out. The default is 15 minutes. The minimum value is five minutes and the maximum value is 2,880 minutes (two days) if the **Token Lifetime** is increased to match the value. If the **Token Lifetime** is not increased, the token will expire before the **Web Client Inactivity Timeout**. When the timeout period is met, a message displays and the user can continue or log out. If there is no response, the user is automatically logged out. The default is 15 minutes.
Lockout Duration	Set the number of minutes a locked out account remains locked. Range: One to 9,999 minutes; A setting of 9,999 requires an administrator to manually unlock the account. Default: 15 minutes
Lockout Threshold	Set the number of consecutive failed sign-in attempts within

	the **Lockout Window** required to lock a user account. If a user submits an incorrect password for the maximum number of times specified by the account **Lockout Threshold** settings within the **Lockout Window**, SPP locks the account until the **Lockout Duration** period has been met. Range: 0 to 100 failed sign-in attempts; A value of 0 (zero) indicates the user's account will never be locked due to failed log ins. The default is five consecutive failures. Set the **Lockout Threshold** to a high enough number that authorized users are not locked out of their user accounts simply because they mistype a password.
Lockout Window	Set the duration (in minutes) in which SPP increments the number of failed sign-in attempts. Range: 0 to 15 minutes; A value of 0 (zero) means that there is no time limit to tracking failed log on attempts. Default: 10 minutes
Deactivate After	Set the number of days to wait before automatically disabling an inactive user account. If a user has not logged onto SPP this number of days, SPP disables the user account. NOTE: The Authorizer Administrator must also reset the user's password when re-enabling a disabled account. Range: 14 to 365 days Default: 365 days
Minimum Password Age	Set the number of days a user must wait before changing their password. Range: 0 to 14 days Default: Zero
Maximum Password Age	Set the number of days users can use their current password before they must change it. Range: 0 to 180 days; A value of 0 (zero) indicates passwords never expire. Default: 42 days
Password Age Reminder	Set the period of time (in days) before the **Maximum Password Age** limit is met and SPP begins to remind the user that their password is about to expire. NOTE: This value will also be applied to any Active Directory Identity and Authentication providers. This only acts as a

	reminder. A user will not be able to change their directory password from within SPP. If an Active Directory user is part of a Fine-Grained Password Policy, that policy's maximum password age setting takes precedence. Range: 0 to 45 days Default: 14 days
Password History	Enter the number of old passwords stored by SPP for user accounts. Stored passwords cannot be reused, and are replaced on a first-in, first-out basis. NOTE: Administrators are not restricted by the password history setting. Range: 0 to 24 old passwords; A value of 0 (zero) disables password history restrictions allowing users to always reuse old passwords. Default: Five stored passwords
Inform User of Locked Account	Select this check box to inform users when SPP has locked their account when they attempt to log in. When cleared, SPP tells the user that their access has been denied. NOTE: For security reasons, One Identity recommends leaving this option cleared, unless you are troubleshooting login and authentication problems. A user with a locked account cannot sign into SPP until the **Lockout Duration** period has been met or an administrator has unlocked the account. For more information, see Unlocking a local user's account on page 549. Default: Not set
Inform User of Deactivated Account	Select this check box to inform users when SPP has disabled their account when they attempt to log in. When cleared, SPP tells the user that their access has been denied. NOTE: For security reasons, One Identity recommends leaving this option cleared, unless you are troubleshooting login and authentication problems. A user with a disabled account cannot sign into SPP until an administrator has re-enabled their account. For more information, see Activating or deactivating a user account on page 548. Default: Not set
Inform User of Bad Password	Select this check box to inform users when the password is bad.

	Default: Not set
Inform User of Expired Password	Select this check box to inform users when the password is expired. Default: Not set
Inform User of Invalid Token	Select this check box to inform users when the token is invalid. Default: Not set
Enable Secure Token Service Login Timeout	Select this check box to set a 15 minute expiration time for session based cookies. Session based cookies are used during login. Typically, a session based cookie does not expire and is deleted by the browser/user-agent when closed. This setting, when enabled, will cause the session-based cookies to have a 15 minute expiration time, enforced by the server. This adds security and can prevent some replay attacks. End users must complete the login process within this time frame, including any multi-factor authentication.

OAuth 2.0 Grant Types

Specify what authorization grants, or flows, the server will allow a client application to use. One Identity recommends to only allow the authorization code grant type with PKCE, which is the default used by Safeguard for Privileged Passwords itself and cannot be disabled. One Identity recommends to disable all other grant types unless you have a custom integration application using them. For backwards compatibility, however, some are enabled by default.

Grant type	Description
Authorization Code	The Authorization Code grant type from the OAuth 2.0 Authorization Framework RFC 6749. This does not enforce the use of the Proof Key for Code Exchange (PKCE) extension, RFC 7636. If you do not have an external application that integrates with Safeguard for Privileged Passwords using this grant type, One Identity recommends that you disable it.
Implicit	The Implicit grant type from the OAuth 2.0 Authorization Framework RFC 6749. If you do not have an external application that integrates with Safeguard for Privileged

Grant type	Description
	Passwords using this grant type, One Identity recommends that you disable it.
Resource Owner	The Resource Owner Password Credential grant type from the OAuth 2.0 Authorization Framework RFC 6749. If you do not have an external application that integrates with Safeguard for Privileged Passwords using this grant type, One Identity recommends that you disable it. NOTE: Some things like the Safeguard-ps PowerShell module may use this grant type when authenticating.
Device Code	The Device Authorization grant type from the OAuth 2.0 extension RFC 8628. This grant type is disabled by default.

Local Password Rule

Password rules define the complexity requirements for user authentication to SPP. You can create rules governing the type of password a user can create, such as:

- Set the allowable password length in a range from 3 to 225 characters.
- Set first characters type and last character type.
- Allow uppercase letters, lowercase letters, numbers, and/or printable ASCII symbols along with the minimum amounts of each.
- Identify excluded uppercase letters, lowercase letters, numbers, and symbols.
- Identify if consecutive letters, numbers, and/or symbols can be repeated sequentially and, if allowed, set the maximum repetitions allowed.

NOTE: These rules only apply to local users; they do not affect users accessing SPP from an external provider such as Microsoft Active Directory. The password rules are listed in the **Set password** dialog. For more information, see Setting a local user's password on page 548.

Modifying user password requirements

It is the responsibility of the Appliance Administrator to configure the user password rules.

To configure user password rules

1. Go to password rules:
   - web client: Navigate to **Safeguard Access** > **Local Password Rule**.
2. Check the current password requirements displayed in the **Rule Summary**.
3. Set the password rule requirements.
   - **Password Length**: Set a range for the password allowable length from three to 255 characters. The default is 8 to 64 characters. The maximum length must be equal to or greater than the sum of minimum characters required in the following steps. For example, if the password must have two uppercase letters, two lowercase letters, and two numeric characters, the minimum **Password Length** must be six. Note that a diacritical letter is one character.
   - **First Character Type**: Choose one of the following:
     - **All**: Alphabetical, numeric, or symbols
     - **Alphanumeric**: Alphabetical or numeric
     - **Alphabetic**: Only alphabetical characters
   - **Last Character Type**: Choose one of the following:
     - **All**: Alphabetical, numeric, or symbols
     - **Alphanumeric**: Alphabetical or numeric
     - **Alphabetic**: Only alphabetical characters
   - **Repeated Characters**: Choose one of the following:
     - **Allow repeated characters**: Any letters, numbers, or symbols can be repeated in any order, including consecutively.
     - **No consecutive repeated characters**: No letter, number, or symbol can be repeated after itself. You can restrict the number of consecutively repeated characters later by uppercase letters, lowercase letters, numbers, symbols, or a combination of those.
     - **No repeated characters**: All letters, numbers, or symbols can only be used once in the password.
   - **Allow Uppercase**: Select to allow uppercase (capital) letters.
     - **Require a Minimum of Uppercase Characters**: Enter a number to identify the least number of uppercase letters required. To allow but not require uppercase letters, set this value at zero.
     - **Limit Consecutively Repeated Uppercase Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated uppercase letters. You must enter a **Maximum Allowed Characters** value of one or more.
     - **Exclude these Uppercase Characters**: Enter any uppercase characters you want to exclude from the password. This field is case-sensitive.

- **Allow Lowercase**: Select to allow lowercase (small) letters.
  - **Require a Minimum of Lowercase Characters**: Enter a number to identify the least number of lowercase letters required. To allow but not require lowercase letters, set this value at zero.
  - **Limit Consecutively Repeated Lowercase Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated lowercase letters. You must enter a **Maximum Allowed Characters** value of one or more.
  - **Excluded these Lowercase Characters**: Enter any lowercase characters you want to exclude from the password. This field is case sensitive.
- **Limit Consecutively Repeated Alpha Characters**: To set the number of repeated lowercase or uppercase letters combined, enter the **Maximum Allowed Characters**.

  For example, if you set the **Max Allowed** at **2** then you can not have more than two alphabet characters next to each other in the password. Using this example, `Ab1Cd2EF` is valid but `AbC1d2EF` is not because it has three alphabet characters in a row.
- **Allow Numeric Character (0-9)**: Select to allow numeric characters in the password.
  - **Require a Minimum of Numeric Characters**: Enter a number to identify the amount of numbers required in a password. To allow but not require numbers, set this value at zero.
  - **Limit Consecutively Repeated Numeric Characters**: Select the check box to limit the number of consecutively repeated numeric characters. You must enter a **Maximum Allowed Characters** value of one or more.
  - **Exclude these Numeric Characters**: Enter any numeric characters you want to exclude from the password. This field is case sensitive.
- **Allow Symbols (e.g. @ # $ % &)**: Select this check box to allow characters that are printable ASCII characters. These often include: ~ ` ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
  - **Require a Minimum of Symbols**: Enter a number to identify the least number of symbols required. To allow but not require symbols, set this value at zero.
  - **Limit Consecutively Repeated Symbols**: If you allowed repeated characters earlier, select the check box to limit the number of symbols that can repeat consecutively. You must enter a **Maximum Allowed Characters** value of one or more.
  - Set the following:
    - **Valid Symbols**: Select this option to enter allowable special characters. Enter the allowable symbols in the **Symbol List** text

box.

- **Invalid Symbols**: Select this option to enter prohibited special characters. Enter the prohibited symbols in the **Symbol List** text box.

4. Click **Test Rule** to check the rules set.
5. When the rules are complete, click **Apply**.

Identity and Authentication

SPP allows you to create various types of identity and authentication providers to integrate with existing directory services. This helps you to effectively manage users and how they will log in to Safeguard. You can create providers for Active Directory, LDAP 2.4, any SAML 2.0 federated service, or Radius.

Go to Identity and Authentication:

- web client: Navigate to **Appliance Management** > **Safeguard Access** > **Identity and Authentication**.

The **Identity and Authentication** pane displays the following details about the identity and authentication providers defined.

Table 62: Identity and Authentication: Properties

Property	Description
Name	The name assigned to the identity or authentication provider. Names are assigned by the administrator that creates the identity or authentication provider. Depending on the provider type, the name may be displayed in a drop-down list on the login page, with exception of Active Directory, External Federation, and any 2FA provider.
Type	Types of identity and authentication providers follow. There are valid primary and secondary authentication combinations. For more information, see Authentication provider combinations on page 256. • Active Directory • LDAP • External Federation • Radius (use as a secondary authentication provider) • Radius as Primary (use as a primary authentication provider) • FIDO2 • OneLogin MFA • SCIM

Property	Description
Description	Enter any descriptive information to use for administrative purposes.
Login Provider ID	A system generated identifier that can be used when integrating with third-party or other custom software or automation scripts. For information on accessing the SPP API, see Using the API. NOTE: When integrating with Safeguard for Privileged Sessions, you can effectively enable Single Sign-On (SSO) between the two applications by creating and using the same SAML2 external federation login provider in both. This **Login Provider ID** value from SPP must then be entered into the Safeguard for Privileged Sessions **Script Reference** field when creating the matching SAML2 login method.

Use these toolbar buttons to manage identity and authentication provider configurations.

Table 63: Identity and Authentication: Toolbar

Option	Description
Add	Add a identity or authentication provider configuration. For more information, see Adding identity and authentication providers on page 259.
Remove	Remove the selected identity or authentication provider. The provider can be deleted if there are no associated users.
Edit	Modify the selected identity or authentication provider.
Syncronize Now	Run the directory addition (incremental) synchronization process for directory users (identity providers) and directory user groups. All changes except for deletions are synced. A **Tasks** window displays the progress and outcome of the task. You can click **Details** to see more information or click **Stop** to cancel the task. The directory deletion and addition (full) synchronization process must be run from the API (`IdentityProviders/Synchronize`).
Update Signing Certificates and Metadata	For external federation providers that have been configured with a URL pointing to the metadata, you can manually trigger SPP to request the metadata from the URL if you know it has changed and don't want to wait for the daily automatic update. This may be necessary in cases where the external STS doesn't support having multiple active signing certificates and you want to minimize any downtime from not being able to log in.
Download Safeguard Federation Metadata	Download a copy of SPP's Federation Metadata XML file. You will need this file to create the corresponding trust relationship on your STS server. The federation metadata XML file typically contains a

Option	Description
	digital signature and cannot be modified in any way, including white space. If you receive an error regarding a problem with the metadata, ensure the file has not been edited.
Refresh	Update the list of identity and authentication providers.

Authentication provider combinations

Some authentication providers can only be used for primary authentication and others can only support secondary authentication. See the table that follows for details on allowable authentication provider combinations.

It is the responsibility of either the Authorizer Administrator or the User Administrator to configure a user account to use two-factor authentication when logging into SPP. For more information, see Requiring secondary authentication log in on page 546.

Using Local as the identity provider

Table 64: Allowable local identity provider combinations

Primary authentication	Secondary authentication
Local: The specified login name and password will be used for authentication.	None OneLogin MFA Radius Active Directory LDAP FIDO2
Certificate: The specified certificate thumbprint will be used for authentication.	None OneLogin MFA Radius Active Directory LDAP FIDO2
External Federation: The specified email address or name claim will be used for authentication.	None OneLogin MFA Radius Active Directory

Primary authentication	Secondary authentication
	LDAP FIDO2
Radius: The specified login name will be used for authentication. NOTE: The Radius server may be configured to integrate with your company's existing identity and authentication solution and may provide its own means of two-factor authentication.	None OneLogin MFA Active Directory LDAP FIDO2

Using Active Directory as the identity provider

Table 65: Allowable Active Directory identity provider combinations

Primary authentication	Secondary authentication
Active Directory: The samAccountName or X509 certificate will be used for authentication. NOTE: The user must authenticate against the domain from which their account exists.	None OneLogin MFA Radius LDAP FIDO2
External Federation: The specified email address or name claim will be used for authentication.	None OneLogin MFA Radius Active Directory LDAP FIDO2
Radius: The specified login name will be used for authentication. NOTE: The Radius server may be configured to integrate with your company's existing identity and authentication solution and may provide its own means of two-factor authentication.	None OneLogin MFA Active Directory LDAP FIDO2

Using LDAP as the identity provider

Table 66: Allowable LDAP identity provider combinations

Primary authentication	Secondary authentication
LDAP: The specified username attribute will be used for authentication.	None OneLogin MFA Radius Active Directory FIDO2
External Federation: The specified email address or name claim will be used for authentication.	None OneLogin MFA Radius Active Directory LDAP FIDO2
Radius : The specified login name will be used for authentication. NOTE: The Radius server may be configured to integrate with your company's existing identity and authentication solution and may provide its own means of two-factor authentication.	None OneLogin MFA Active Directory LDAP FIDO2

Using Starling as the identity provider

Table 67: Allowable Starling identity provider combinations

Primary authentication	Secondary authentication
Starling	None

Using SCIM as the identity provider

Table 68: Allowable SCIM identity provider combinations

Primary authentication	Secondary authentication
Local: The specified username and password will be used for	None

Primary authentication	Secondary authentication
authentication. NOTE: A SPP user administrator must manually set the password for any newly provisioned SCIM users.	OneLogin MFA Radius Active Directory LDAP FIDO2
External Federation: The specified email address or name claim will be used for authentication.	None OneLogin MFA Radius Active Directory LDAP FIDO2

Adding identity and authentication providers

It is the responsibility of the Appliance Administrator to add directories to Safeguard for use as identity and authentication providers.

If Active Directory forests have more than one domain, select the domain to use for identity and authentication and to display on the logon screen. It is the responsibility of an Appliance Administrator to create an External Federation or Radius provider to use for authentication.

To add identity and authentication providers

1. Go to Identity and Authentication:
   - web client: Navigate to **Safeguard Access** > **Identity and Authentication**.
2. Click **Add**.
3. Click the provider:
   - Active Directory: See Active Directory and LDAP settings.
   - LDAP: See Active Directory and LDAP settings.
   - External Federation: See External Federation settings.
   - Radius: See Radius settings.
   - FIDO2: See FIDO2 settings.
   - OneLogin MFA: See OneLogin MFA settings.
   - SCIM: See SCIM settings.

Active Directory and LDAP settings

Use the **General** tab to add the required service account information. The following table lists the properties and designates the properties for Active Directory and LDAP.

Table 69: Active Directory and LDAP: General tab properties

Property	Description
Product	The product name.
Forest Root Domain Name	Forest Root Domain Name.
Name	Unique name.
Service Account Domain Name (for Active Directory)	Enter the fully qualified Active Directory domain name, such as `example.com`. Do not enter the domain controller hostname, such as `server.example.com`; the domain controller's IP address, such as `10.10.10.10`; or the NETBIOS domain name, such as `EXAMPLE`. The service account domain name is the name of the domain where the service account resides. SPP uses DNS-SRV to resolve domain names to actual domain controllers.
Network Address (for LDAP)	Enter a network DNS name or the IP address of the LDAP server for SPP to use to connect to the managed system over the network.
Service Account Name (for Active Directory)	Enter an account for SPP to use for management tasks. If the Active Directory has previously been added as an asset, you can use the same service account, but you will need to know the current password of the account. Once added, you can have SPP manage the service account and periodically change the password without effecting the connectivity. For identity and authentication purposes, the service account only requires read access to the Active Directory domain(s). The service account does not require write access. Typically, any member of the default Domain Users group is sufficient. The service account must be able to read the following attributes on all users: • objectGuid • objectSID • userPrincipalName • samAccountName • displayName • mail

Property	Description
	• userAccountControl • pwdLastSet • msDS-ResultantPSO • tokenGroups • lockoutTime • accountExpires In addition, the service account requires read access to other domain level attributes: • dnsHostName • defaultNamingContext • rootDomainNamingContext • configurationNamingContext • schemaNamingContext • nETBIOSName • nCName • ldapDisplayName • maxPwdAge • lockoutDuration • msDS-MaximumPasswordAge • msDS-LockoutDuration Lastly, the service account must be able to enumerate the Active Directory User object class hierarchy to build the complete attribute schema. For more information, see About service accounts on page 321.
Service Account Distinguished Name (for LDAP)	Enter a fully qualified distinguished name (FQDN) for SPP to use for management tasks. For example: `cn=dev-sa,ou=people,dc=example,dc=com`
Service Account Password	Enter the password SPP uses to authenticate to this directory.
Description	Enter information about this external identity provider.
Connect	Click **Connect** to verify the credentials. If adding an Active Directory provider, all domains in the forest will be displayed. Choose which ones can be used for identity and authentication.
Available Domains for Identity and	All newly created Safeguard users that are imported from the directory user group will have their primary authentication

Property	Description
Authentication (for Active Directory)	provider set to use the directory domain from which their user originates. For an Active Directory forest with multiple domains, the domains must be marked as **Available Domains for Identity and Authentication**. Clearing the forest root domain will have undesired results when managing directory users and groups. For more information, see Adding a directory user group on page 556.
Advanced	Open to reveal the following synchronization settings:
Port (for LDAP)	Enter port 389 used for communication with the LDAP directory.
Use SSL Encryption	Select whether or not to use SSL when connecting to the server. You must have a valid SSL certificate and have the SSL's issuer certificate be trusted by SPP. For more information, see Trusted CA Certificates.
Domain Controllers	For Active Directory, instead of having SPP automatically find domain controllers from a DNS and CLDAP ping, you can specify domain controllers.
Sync additions every	Enter or select how often you want SPP to synchronize directory additions (in minutes). This updates SPP with any additions, or modifications that have been made to the directory objects, including group membership and user account attributes mapped to SPP. Default: 15 minutes Range: Between 1 and 2147483647
Sync deletions every	Enter or select how often you want SPP to synchronize directory deletions (in minutes). This updates SPP with any deletions that have been made to the directory objects, including group membership and user account attributes mapped to SPP. Default: 15 minutes Range: Between 1 and 2147483647

Attributes tab

On the **Attributes** tab, synchronize the attributes in SPP to the directory schema attributes. The **Attributes** tab displays the default directory attributes that are mapped to the SPP properties, such as the user's first name.

There are multiple valid schema mappings supported and you can modify its configuration, as needed. For example, the **LDAP** dialog, **Attributes** tab may display the **Username** as the cn <Display Name> or the uid <Username> based on your directory configuration.

To map the SPP properties to different directory attributes

1. **Browse** to select one or more object classes for the users, computers, and groups categories, as applicable.

   NOTE: You can use or remove the default object class.

2. If you do not want to use the default property, begin typing in the property box. SPP' auto-complete feature immediately displays a list of attributes to choose. SPP only allows you to select attributes that are valid for the object classes you have selected for users, groups, and computers.
3. Once you have set all the properties, click **Apply**.

The following table list the default directory attributes.

Table 70: Active Directory and LDAP: Attributes tab (defaults)

SPP attribute	Directory attribute
Users	
Object Class	**Browse** to select a class definition that defines the valid attributes for the user object class. Default: `user` for Active Directory, `inetOrgPerson` for LDAP
User Name	`sAMAccountName` for Active Directory, `cn` for LDAP
Password	`userPassword` for LDAP
First Name	`givenName`
Last Name	`sn`
Work Phone	`telephoneNumber`
Mobile Phone	`mobile`
Email	`mail`
Description	`description`
External Federation Authentication	The directory attribute used to match the email address claim or name claim value from the SAML Response of an external federation authentication request. Typically, this will be an attribute containing the user's email address or other unique identifier used by the external Secure Token Service (STS). For both Active Directory and LDAP 2.4, this will default to the "mail" attribute. This is only used when processing members of a directory user group in which the group has been configured to use an External Federation provider as the primary authentication. For more information, see Adding a directory user group on page 556.

SPP attribute	Directory attribute
Radius Authentic-ation	The directory attributed used to match the username value in an external Radius server that has been configured for either primary or secondary authentication. For Active Directory, this will default to using the `samAccountName` attribute. For LDAP 2.4, this will default to using the `cn` attribute. NOTE: This is only used when processing members of a directory user group in which the group has been configured to use Radius as either the primary or secondary authentication provider. For more information, see Adding a directory user group on page 556.
Managed Objects	The directory attribute used when automatically associating existing managed Accounts to users of a directory user group as linked accounts. Defaults: • For Active Directory, this defaults to `managedObjects`. However, you may want to use the `directReports` attribute based on where you have the information stored in Active Directory. • For LDAP 2.4, this defaults to the `seeAlso` attribute. When choosing an attribute, it must exist on the user itself and contain one or more `Distinguished Name` values of other directory user objects. For example, you would not want to use the `owner` attribute in LDAP 2.4, as the direction of the relationship is going the wrong way. You would instead want an owns attribute to exist on the user such as the default `seeAlso` attribute. For more information, see Adding a directory user group on page 556.
Groups	
Object Class	**Browse** to select a class definition that defines the valid attributes for the group object class. Default: `group` for Active Directory, `groupOfNames` for LDAP
Name	`sAMAccountName` for Active Directory, `cn` for LDAP
Member	`member`
Description	`description`

External Federation settings

One Identity Safeguard for Privileged Passwords supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different STS servers and services, such as Microsoft's AD FS. Through the exchange of the federation metadata,

you can create a trust relationship between the two systems. Then, you will create a SPP user to be associated with the federated user. When an end user logs in, they will be redirected to the external STS to enter their credentials and perform any two-factor authentication that may be required by that STS. After successful authentication, they will be redirected back to SPP and logged in.

NOTE: Additional two-factor authentication can be assigned to the associated SPP user to have the user authenticate again after being redirected back from the external STS.

To use external federation, you must first download a copy of, or have the URL to the federation metadata XML of your STS. For example, in Microsoft AD FS, you can download the federation metadata XML from: `https://<adfs server>/FederationMetadata/2007-06/FederationMetadata.xml`. Or if the Safeguard for Privileged Passwords appliance can directly access that URL, it can be used as well when creating the provider.

To add external federation:

1. In the **External Federation** dialog, supply the following information:
    a. **Name**: The unique name assigned to the external federation service provider. The name is for administrative purposes only and will not be seen by the end users.
    b. **Description**: Enter any text. The text is seen only here and used for administrative purposes.
    c. **Realm**: Enter a unique realm value, typically a DNS suffix, like `contoso.com`, that matches the email addresses of users intended to use this STS for authentication. Values can be separated by a space, comma, or semi-colon. A case-insensitive comparison will be used on the value(s) when performing Home Realm Discovery.
    d. Federation Metadata: Select one of the following options:
        i. **From File**: When using this option, SPP stores a static copy of the metadata. It is the responsibility of the administrators to update the metadata, when necessary, by repeating this process. For example, when the signing certificate used by the STS changes.

        You must first download the federation metadata XML for your STS and save it to a file locally. For example, for Microsoft's AD FS, you can download the federation metadata XML from: `https://<adfs server>/FederationMetadata/2007-06/FederationMetadata.xml`.

        Click **Browse** to select the STS federation metadata xml file.

        ii. **From URL**: When using this option, SPP will automatically download the STS metadata and refresh it on a periodic basis, so it should always have the current signing certificates and other information used by the STS.

        Specify the complete HTTPS URL to the STS metadata. The SSL/TLS certificate used by the HTTPS URL must be trusted on every node of the SPP cluster, and each node of the cluster will need network/internet access to be able to download from the specified HTTPS URL. It is strongly recommended to verify that you can successfully log in on each node of the cluster after initially creating the Identity Provider.

After the external federation provider is created, you can manually trigger SPP to update the metadata from the configured URL by clicking the **Update Metadata** button. This may be useful to help minimize any downtime when you know that the STS metadata has changed.

> NOTE: A proxy server may be configured. For more information, see Networking.

e. **Application ID Override**: If needed, override the **Issuer name** value that is sent in a SAML2 AuthnRequest to match the ID of the relying party application defined in the IdP.

   For example, when creating an App registration in Microsoft's Azure AD, you would copy the Application ID URI value into this field.

f. **Login Provider ID**: A system generated identifier that can be used when integrating with third-party or other custom software or automation scripts. For information on accessing the SPP API, see Using the API.

   > NOTE: When integrating with Safeguard for Privileged Sessions, you can effectively enable Single Sign-On (SSO) between the two applications by creating and using the same SAML2 external federation login provider in both. This **Login Provider ID** value from SPP must then be entered into the Safeguard for Privileged Sessions **Script Reference** field when creating the matching SAML2 login method.

g. When the **Require User to Always Authenticate** check box is selected, the user will always be required to enter their credentials on the external provider, regardless of whether they are already logged in. This may be seen as negating one of the features of Single Sign-On, and therefore can be turned off. Or it may be considered a more secure option and turned on.

2. Click **Download SPP Metadata File**: You will need this file to create the corresponding trust relationship on your STS server. The federation metadata XML file typically contains a digital signature and cannot be modified in any way, including white space. If you receive an error regarding a problem with the metadata, ensure the file has not been edited. Also see: How do I create a relying party trust for the STS.

Radius settings

Create and configure a Radius server for use as either a primary authentication provider or secondary authentication provider. To use a Radius server for both primary and secondary authentication, you will need to create two authentication providers. The steps to create Radius as a primary provider or secondary provider follow:

1. In the **Radius** dialog, supply the following information:

   a. **Name**: The unique display name. When creating the Radius provider for primary authentication, this name value will be displayed in the drop-down list on the login page.

   b. **Description**: Enter any text. The text is seen only here and used for administrative purposes.

c. **Type**: Choose **As Primary Authentication** or **As Secondary Authentication**.

d. **Server Address**: Enter a network DNS name or the IP address used to connect to the server over the network.

e. **Secondary Server Address**: (Optional) Enter a network DNS name or the IP address for an additional or redundant server.

f. **Shared Secret**: Enter the server's secret key. Click to show the server's secret key.

g. **Port**: Enter the port number that the Radius server uses to listen for authentication requests. The default is port 1812.

h. **Timeout**: Specify how long to wait before a Radius authentication request times out. The default is 20 seconds.

i. **PreAuthenticate for Challenge/Response**: If selected, an `Access-Request` call containing only the `User-Name` is sent to the Radius server prior to the user's authentication attempt. This is done to inform the Radius server of the user's identity so it can possibly begin the authentication process by starting a challenge/response cycle. This may be required to seed the user's state data. In addition, the Radius server's response may include a login message that is to be displayed, which is specific to that user.

   If the Radius server is not configured to respond with an `Access-Challenge`, then this will cause the log in to fail and the user will be unable to proceed. This setting is only applicable when using Radius as a secondary authentication provider. The setting has no effect if enabled on a primary authentication provider.

j. **Always Mask User Input**: If selected, the text box that the user enters their one-time password, or other challenge required by the Radius server, will always be a password style text box in which the user's input is masked and appears as a series of dots, not as clear text. This may be desired when the challenge is not only a one-time password, but also contains the user's PIN. This will prevent any passer-by from seeing the private information. Note, however, that when this setting is enabled, it will also override the Prompt attribute of the Radius server's `Access-Challenge` response, such that the user's input will always be masked.

2. Click **OK**.

NOTE: When SPP attempts to authenticate a user against the Radius server, it will always include the `NAS-Identifier` Radius attribute with a value set to the appliance ID. There is no setting to turn this on or off, nor specify a custom value.

FIDO2 settings

Create and configure FIDO2 for use as a secondary authentication provider.

1. In the FIDO2 dialog, provide the following settings:

   a. **Name**: The unique name assigned to the provider. The name is for administrative purposes only and will not be seen by the end users.

b. **Domain Suffix**: This must be a DNS name that identifies the appliance. Typically, this will be the DNS name used to access Safeguard. It cannot be an IP address. The value is a a domain string identifying the WebAuthn Relying Party for which the registration or authentication ceremony is performed.

   A public key credential can only be used for authentication with the same entity (identified by this value) it was registered with. However, this value can be a registerable domain suffix of what appears in the user's browser when registering. For example, you could enter `contoso.com` to register against a server at `https://www.contoso.com` or `https://node1.contoso.com`. Later, you can use the same authenticator security key to authenticate at either of the locations.

c. **Description**: Enter any text. The text is seen only here and used for administrative purposes.

2. Click **OK**.

OneLogin MFA settings

Create and configure OneLogin MFA as a secondary authentication provider.

IMPORTANT: Before configuring OneLogin as an authentication provider, you must first purchase a subscription with OneLogin.com and create an API credential to be used by SPP. For information on OneLogin, see OneLogin documentation.

NOTE: The OneLogin administrative site is used to configure the desired Authentication Factors, security policies, and users. SPP currently supports the following secondary authentication methods:

- OneLogin Protect
- Authenticator
- SMS
- Email

1. In the OneLogin MFA dialog, provide the following settings:

   a. **Name**: The unique name assigned to the provider. The name is for administrative purposes only and will not be seen by the end users (up to 50 characters).

   b. **Description**: Enter any text. The text is seen only here and used for administrative purposes (up to 255 characters).

   c. **DNS Host Name**: Enter the complete OneLogin DNS host name of your subscription; for example, `<subdomain>.onelogin.com`.

   d. **Client ID**: Enter the API Client ID created in OneLogin. SPP requires that the **Manage All** permission is used for the API credentials created in OneLogin. For more information, see Working with API Credentials.

   e. **Client Secret**: Enter the API Client Secret created in OneLogin. SPP requires that the **Manage All** permission is used for the API credentials created in OneLogin. For more information, see Working with API Credentials.

2. Click **OK**.

NOTE: After you have configured OneLogin MFA as an authentication provider, when adding individual users to SPP you need to ensure the email address configured for that user is identical to what is in OneLogin. After initial configuration, the user information in OneLogin can be updated if needed without impacting the connection with SPP.

SCIM settings

Create and configure System for Cross-Domain Identity Management (SCIM) provisioning via Azure Active Directory or OneLogin.

IMPORTANT: To configure SCIM provisioning in Azure Active Directory you must use an account with the Global Admin role. For more information on SCIM provisioning, see SCIM synchronization with Azure Active Directory.

1. In the SCIM dialog, provide the following settings:
   a. **Name**: The unique name assigned to the provider. The name is for administrative purposes only and will not be seen by the end users.
   b. **Description**: Enter any text. The text is seen only here and used for administrative purposes.
2. Click **OK** to save the information.
3. On the **Identity and Authentication** pane, select the name of the newly created SCIM provider and click .
4. Use the **General** tab to provide the following information:

Table 71: SCIM: General tab

Setting	Description
Name	The unique name assigned to the provider. The name is for administrative purposes only and will not be seen by the end users.
Description	Enter any text. The text is seen only here and used for administrative purposes.
Tenant URL	This is the URL for the tenant that you specified in Azure Active Directory. Use the button to copy the URL.
Application Token	This is the token required to connect with Azure Active Directory and will needed to be added to you SCIM provisioning configuration in Azure Active Directory. Use the **Generate New Token** button to populate this field and provide a button to copy the token. The token text for a previously generated token is unavailable for both viewing and copying once you save the configuration.
Application Token Set	This is the date (month, day, year) that the token was last generated.

Setting	Description
Generate New Token	Click this button to generate a new token. Once generated, the token text will appear in the **Application Token** field.

5. Use the **Authentication** tab to provide the following information:

Table 72: SCIM: Authentication tab

Setting	Description
Default Primary Authentication Provider	(Optional) Select a primary authentication provider.
Default Secondary Authentication Provider	(Optional) Select a secondary authentication provider.

6. On the **Permissions** tab, select any of the administrative permissions and/or the **Personal Password Vault** permission to be assigned to each member of the **SCIM User Group**. For each group member, the selected permissions of the group will be combined with any existing permissions that have already been granted explicitly or by some other Group to which they belong. For more information, see the Permissions tab (add user).
During synchronization of a SCIM User Group, a user may be identified as no longer being a member. In this case, the selected permissions of the SCIM User Group are removed from the user unless the user is also a member of another Group from which they inherit the permission. SPP does not keep track of nor distinguish between an explicitly assigned permission versus one that was assigned via a Group.
7. IMPORTANT: The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Groups from which they inherited it, the user will no longer be able to access **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission again, they regain access to all of their existing data.
8. Click **OK**.

Branding Customization

The Appliance Administrator can customize the login page and application for their users. Any customization must be configured on the primary, however any customization will also appear on replicas.

To customize the branding used on the login page and application header

1. Navigate to **Appliance Management** > **Safeguard Access** > **Branding**.
2. Select **Custom Branding**.
3. In the **Login Page** section, the **Title** field allows you to enter a name for the application (up to 50 characters long) that will appear on the login page.
4. For the **Title Size**, enter the font size in pixels to use for the application name. By default this is 36 px.
5. To customize the display colors, click the box beneath each field name to open a color selector dialog:
   a. **Title Color**
   b. **Background Color**
   c. **Page Text Color**
6. Click the **Upload Logo** button to select a logo file to use for the login page (256KB max file size; recommended width: 160px to 400px, height 160px to 200px). Once uploaded, the uploaded logo will be displayed beneath the **Page Text Color** field.
7. In the **Application Header** section, the **Title** field allows you to enter the display name (up to 50 characters long) that will be used within the header of the application.
8. Click the **Upload Logo** button to select a logo file to use within the header of the application (256KB max file size; recommended width: 48px to 150px, height 48px to 64px). Once uploaded, the uploaded logo will be displayed beneath the **Title** field.
9. Click **Save**.

   After saving, you can view the changes using the **Review Login Page Customization** or **Review Application Customization** buttons.

NOTE: You can select the **Safeguard Branding** option at the top of the page and click **Save** to remove any configured customizations and restore the SPP branding. After clicking **Save** you will be prompted for confirmation.

Appliance Management Settings

In the web client, **Appliance Management** has a settings page used to manage the maximum number of platform task retries.

Navigate to **Appliance Management** > **Settings** to manage the setting listed below.

Table 73: Appliance Management Setting

Setting	Description
Maximum Platform Task Retries	Set the maximum number of platform retries.

11

Asset Management

In the web client, expand the **Asset Management** section in the left navigation pane.

Account Automation

Also available as a pane on the **Home** page, the **Asset Management** > **Account Automation** page allows Asset Administrators to view information regarding accounts that are failing or succeeding different types of tasks. This page includes both automated and manual tasks in the results. Clicking one of the tasks on the view displays additional information.

Click the button to customize the tasks that are displayed.

Account Automation: Toolbar

After selecting a task to view additional information, use the toolbar at the top of the details grid to perform the following tasks.

- **View Details**: After selecting a task from the table, click this button to view additional information on the task.
- **Re-Run Task**: Available for failed tasks only, select to rerun the selected task.
- **Remove**: Available for failed tasks only, select to remove the selected task.
- **Export**: Select to create a .csv or .json file of the currently displayed account automation grid and save it to a location of your choice. For more information, see Exporting data.
- **Refresh**: Select to refresh the data displayed in the table.
- **Columns**: Select to display a list of columns that can be displayed in the grid. Select the check box for data to be included in the grid. Clear the check box for data to be excluded from the grid.

Accounts

A SPP account is a unique identifier that SPP uses to control access to assets. Managed accounts (including directory accounts and service accounts) and groups of accounts can be associated with an asset. Each account has an associated asset; if you delete an asset, SPP permanently deletes all the accounts associated with it.

The Auditor and the Asset Administrator have permission to access **Accounts**.

On Unix assets, the accounts are stored in `etc/passwd`; however, each platform implements this concept differently.

Service accounts are designated with a **Service Account** icon. For more information, see About service accounts.

To access **Accounts**, in the web client, navigate to **Asset Management** > **Accounts**. If needed, you can use the partition drop-down to select the parent partition of the account. Select an account, then click to display additional information and options.

Selecting one of the accounts displays the following information:

- Properties (account): Displays general information about the selected account. It also allows you to manage Passwords, SSH keys, API keys, and TOTP authenticators for the account.
- Owners tab (account): Displays information about the owners of the account.
- Dependent Assets (account): (Directory assets) Displays the assets that have dependency on the selected directory account. This tab only displays for a directory asset and displays the assets that have dependency on the selected directory account.
- Check and Change Log tab (account): Displays the password and SSH key validation and reset history for the selected account.
- Discovered Services tab (account): (Windows and Active Directory accounts) Displays information on the services dependent to a selected account.
- Discovered SSH Keys (account): Displays the SSH keys discovered on the account.
- History tab (account): Displays the details of each operation that has affected the selected account.

For information about configuring Account Discovery in SPP, see Account Discovery job workflow.

Use these toolbar buttons to manage accounts.

- **+ New Account**: Add accounts to SPP. Adding an account.
- **Delete**: Remove the selected account. Deleting an account.
- **View Details**: Select an account then click this button to open additional information and options for the account.
- **Account Secrets**: Possible menu options include:

    - **Check Password**
    - **Change Password**
    - **Check SSH Key**
    - **Change SSH Key**
- **Access Request**: Allows you to enable or disable access request services for the selected account. Menu options include:
    - Enable Password Request
    - Disable Password Request
    - Enable Session Request
    - Disable Session Request
    - Enable SSH Key Request
    - Disable SSH Key Request
    - Enable API Key Request
    - Disable API Key Request
- **Discover SSH Keys**: Run the SSH Key Discovery job.
- **Show Disabled**: Display the accounts that are not managed and are disabled and have no associated assets.
    - Click **Disable** to prevent SPP from managing the selected account.
    - Click **Enable** to manage the selected account and assign it to the scope of the default profile.
- **Hide Disabled**: Hide the accounts that are not managed and are disabled and have no associated assets.
    - Click **Disable** to prevent SPP from managing the selected account.
    - Click **Enable** to manage the selected account and assign it to the scope of the default profile.
- **Import**: Click this to open a drop-down menu from which you can select to add accounts, passwords, or SSH keys to One Identity Safeguard for Privileged Passwords using a CSV file. For more information, see Importing objects.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of accounts.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Properties (account)

The **Properties** tab lists information about the selected account.

To access **Properties**:

- web client: Navigate to **Asset Management** > **Accounts** > (View Details) > **Properties**.

Information for the account displays. Not all the information listed below is applicable for every account.

The following options are available on the top of the **Properties** tab:

- **Discover SSH Keys**: Use this option to run the selected SSH Key Discovery job.
- **Enable-Disable**: Select one of the following:

  Select **Enable** to have SPP manage a disabled asset. Account Discovery jobs find all accounts that match the discovery rule's criteria regardless of whether it has been marked **Enabled** or **Disabled** in the past.

  Select **Disable** to prevent SPP from managing the selected asset. When you disable an asset, SPP disables it and removes all associated accounts. If you choose to manage the asset later, SPP re-enables all the associated accounts.

The following fields and options display on the secondary tabs on the **Properties** tab based on the type of asset (for example, Windows, Linux, LDAP, or Active Directory). Clicking the **Edit** button on one of the secondary tabs allows you to edit the account.

Table 74: Accounts Properties tab: General properties

Property	Description
Name	The name of the selected account.
Description	Description of the selected account.
Asset	The display name of the managed system associated with this account. Accounts are only associated with one asset.

Table 75: Accounts Properties tab: Management properties

Property	Description
Access Requests	Indicates which type(s) of access requests are enabled for this account.
Password Profile	The name of the password profile that governs the accounts assigned to a partition. When a password profile is inherited from an asset or partition this will be indicated by the text `(Inherited)` next to the name of the password profile. When the password profile is explicitly set, a button will appear that allows you to clear the explicitly set password profile and instead use the inherited password profile.
SSH Key Profile	The name of the SSH key profile.

Property	Description
	When an SSH key profile is inherited from an asset or partition this will be indicated by the text `(Inherited)` next to the name of the SSH key profile. When the SSH key profile is explicitly set, a ✕ button will appear that allows you to clear the explicitly set SSH key profile. Once the cleared profile change is applied, the assigned inherited profile will be displayed. If there is no default SSH key profile designated for the partition, the asset will no longer have an SSH key profile assigned. If there is no SSH key profile explicitly set on the asset, the accounts on that asset will no longer have an SSH key profile assigned. Designating a default SSH key profile for the partition will ensure all assets and accounts in that partition have an inherited SSH key profile.

Table 76: Accounts Properties tab: Secrets properties

Property	Description
Passwords	This tile is for managing the password for the account. The following options are available from the tile: • **View Archive**: Available once a password has been set, clicking this link displays previously assigned passwords for the selected asset. This dialog does not display the current password for the asset. The password archive is never purged. For more information, see Viewing password archive. • **Set**: Click this button to set the account password in the SPP database. The **Set** option does not change the account password on the asset. • **Check**: Click this button to verify the account password is in sync with the SPP database. If the password verification fails, you can change it. • **Change**: Click this button to reset and synchronize the account password with the SPP database. For more information, see Checking, changing, or setting an account password.
TOTP Authenticator	This tile is for managing the TOTP Authenticator for the account. The following options are available from the tile: • **Set**: Click this button to set the TOTP Authenticator. For more information, see Setting a TOTP authenticator. • **Remove**: Click this button to remove a previously configured TOTP Authenticator. For more information,

Property	Description
	seeSetting a TOTP authenticatorRemoving a TOTP authenticator.
SSH keys	This tile is for managing the SSH keys for the account. The following options are available from the tile: • **View Archive**: Available once an SSH key has been set, clicking this link displays previously assigned SSH keys for the selected asset. This dialog does not display the current SSH key for the asset. The SSH key archive is never purged. For more information, see Viewing SSH key archive. • **Set**: Click this button to set the SSH key in the SPP database. The **Set** option does not change the account SSH key on the asset. • **Check**: Click this button to verify the account SSH key is in sync with the SPP database. If the SSH key verification fails, you can change it. • **Change**: Click this button to reset and synchronize the SSH key with the SPP database. For more information, see Checking, changing, or setting an SSH key.
API keys	Viewing API Key Archive • **New API Key**: Click this button to add a new API key to an account. For more information, see Adding an API key. Each API key configured for the account will have a tile containing the following options: NOTE: Should 4 or more API keys be configured, the tiles will be condensed into a single summary tile. To access and manage the individual API keys, click the name of the tile (**API Keys <*n*>**). This will open a pane containing a table view of the configured API keys as well as toolbar options for managing the keys. • **View Archive**: Click this link to access an archive of the API Key. For more information, see Viewing API Key Archive. • **Set**: Click this button to set the API key in the SPP database. The **Set** option does not change the account SSH key on the asset. • **Check**: Click this button to verify the account SSH key is in sync with the SPP database. If the SSH key verification fails, you can change it. • **Change**: Click this button to reset and synchronize the SSH key with the SPP database.

Property	Description
	• (Remove): Click this button to remove a previously configured API Key. For more information, see Checking, changing, or setting an API key.

Tags: Tag assignments for the selected account.

The information displayed in the **Tags** pane includes both the dynamic tags added through tagging rules and static tags that were added manually. In addition to viewing tag assignments, Asset Administrators can add and remove statically assigned tags.

Delete: Click this button to delete the selected account.

Owners tab (account)

The **Owners** tab displays information about the owners associated with the account (and its associated assets). For more information on altering the owners assigned via tags, see Modifying an asset or asset account tag.

To access **Owners**:

- web client: Navigate to **Asset Management** > **Accounts** > (View Details) > **Owners**.

The Owners tab has three views: **Account Owners**, **Asset Owners**, and **Partition Owners**.

Table 77: Accounts: Owners tab properties

Property	Description
Account Owners	
Type	The type of owner.
Name	The name of the owner.
Provider	The name of the authentication provider.
Direct	This column indicates the ownership of the object was assigned directly rather than through the use of a tag.
Via Tag	This column indicates the ownership of the object was assigned through the use of a tag.
Asset Owners	
Type	The type of owner.

Property	Description
Name	The name of the owner.
Provider	The name of the authentication provider.
Direct	This column indicates the ownership of the object was assigned directly rather than through the use of a tag.
Via Tag	This column indicates the ownership of the object was assigned through the use of a tag.
Partition Owners	
Type	The type of user or group.
Name	The name of the user or group.
Provider	The name of the authentication provider.

Use the following buttons on the details toolbar to manage the objects owned by the selected account.

Table 78: Accounts: Owners toolbar

Option	Description
Add	Add one or more users or user groups to the selected account. For more information, see Adding users or user groups to an account.
Remove	Remove the selected object from being a manager of the selected account. You can only remove objects directly assigned to an account (as opposed to those assigned via the use of a tag).
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of owners/managers.
Search	To locate a specific object in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78..

Dependent Assets (account)

The **Dependent Assets** tab only displays for a directory account and displays the assets that have dependency on the selected directory account. Adding account dependencies.

To access **Dependent Assets**, in the web client, navigate to **Asset Management** > **Accounts** > **View Details** > **Dependent Assets**.

Table 79: Accounts: Dependent Assets tab properties

Property	Description
Name	The Windows asset name.
Network Address	The network DNS name or IP address of the managed system.
Platform	The platform of the selected managed system.
Asset Partition	The partition where the Windows asset is assigned.

Use these buttons on the details toolbar to manage the dependent assets.

Table 80: Accounts: Dependent Assets tab toolbar

Option	Description
Refresh	Update the list of dependent assets assigned to the selected account.
Search	To locate a specific dependent asset in this list, enter the character string to be used to search for a match. For more information, see For more information, see Search box on page 78..

Access Request Policies (account)

The **Access Request Policies** tab displays the entitlements and access request policies, including password and SSH key release policies and session request policies, associated with the selected account. This information is available to users that have both Asset Administrator and Policy Administrator permissions.

To access **Access Request Policies**, in the web client, navigate to **Asset Management** > **Accounts** > **View Details** > **Access Request Policies**.

Table 81: Accounts: Access Request Policies tab properties

Property	Description
Entitlement	The name of the access request policy's entitlement.
Access Request Policy	The name of the access request policy that governs the selected account.
Accounts	The number of unique accounts in the account groups that are associated with the access request policy.
# Account Groups	The number of unique account groups in the access request policy.
Account Groups	The names of the account groups that associate the selected account with the policy.

Property	Description
Assets	The number of unique assets in the asset groups that are associated with the access request policy.
# Asset Groups	The number of unique assets groups in the access request policy.
Asset Groups	The names of the asset groups that associate the selected account with the policy.

Use these buttons on the details toolbar to manage the dependent assets.

Table 82: Accounts: Access Request Policies tab toolbar

Option	Description
+ Add to Policy	Add the selected account to the scope of an access request policy.
−Remove Selected	Remove the selected policy.
Refresh	Update the list of dependent assets assigned to the selected account.
Search	To locate a specific dependent asset in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78..

Check and Change Log tab (account)

The **Check and Change Log** tab displays the password and SSH key validation and reset history for the selected account.

By default, the check and change log entries displayed are for the last 24 hours. On the web client, use the **Date Range** drop-down to select a time frame to display and use **Export** to export the listed data as either a JSON or CSV file (for more information, see Exporting data). If the display does not refresh after selecting a different time interval, click the **Refresh**.

To access **Check and Change Log**:

- web client: Navigate to **Asset Management** > **Accounts** > (View Details) > **Check and Change Log**.

Table 83: Accounts: Check and Change Log tab properties

Property	Description
User	The display name of the user that triggered the event

Property	Description
Status	The status of the transaction: • Failure • Success • Queued
Reason	A system message pertaining to the password and SSH key validation and reset activity, such as the password matches the asset, was changed successfully, or does not match the asset.
Type	The type of transaction: • Check Password • Change Password • Check SSH Key • Change SSH Key NOTE: **Check and Change Log** only displays events that the appliance performs; that is, it only displays check and change transactions. It does not display Set Password or Set SSH Key transactions. See: • Checking, changing, or setting an account password • Checking, changing, or setting an SSH key
Date/Time	The date of the transaction. The time stamps for transactions are based on the user's local time.
Duration	The amount of time the transaction took to complete.

Discovered Services tab (account)

The **Discovered Services** tab displays information on the services dependent to a selected account. This tab is only available for Windows and Active Directory accounts.

To access **Discovered Services**, in the web client, navigate to **Asset Management** > **Accounts** > ✎ **View Details** > **Discovered Services**.

Use these buttons to manage the discovered services.

Table 84: Discovered Services: Toolbar

Option	Description
▶ **Discover Services**	Run the discover services task for each unique Windows asset in the grid below.

Option	Description
	IMPORTANT: Before running a service discovery job, ensure you have used unique names for the services. Services with identical names but different service types may not be accurately discovered. For example, an account/asset using the name `test1` that appears under both Windows and Windows SSH will only return one discovery result despite there being 2 asset-s/accounts.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of service discovery jobs.
Search	To locate one or more assets, enter the character string to be used to search for a match. Click **Search**, and select an attribute to search on or type in a colon and the attribute text string for one or multiple attributes. For more information, see For more information, see Search box on page 78..

The following displays for each discovered service.

Table 85: Accounts: Discovered Services tab properties

Property	Description
Asset Name	The name of the Windows asset.
Partition	The name of the partition associated with the Windows asset.
Dependent Account	A ✔ check displays if the account is associated as an account dependency on the asset. The value is blank if the account is not associated as an account dependency of the asset.
Service Type	Type of service discovered. Values may be **Service** or **Task**.
Service Name	The name of the discovered service or task.
Service Enabled	A ✔ check displays if the service or task on the asset is enabled. If there is no check mark, the service or task is disabled.
Discovered Account	The discovered service account name configured.
Date/Time Discovered	The date and time when the service or task was discovered.

Discovered SSH Keys (account)

The **Discovered SSH Keys** tab displays the discovered SSH keys for the account.

To access **Discovered SSH Keys**, in the web client, navigate to **Asset Management** > **Accounts** > ✎ **View Details** > **Discovered SSH Keys**.

Table 86: Accounts: Discovered SSH Keys tab properties

Property	Description
Fingerprint	The fingerprint of the SSH key used for authentication.
Account Status	The status of the Safeguard account.
SSH Key Managed	This column will have a check mark indicating the SSH key currently in use on the account.
Comment	Free form comment.
Key Type	SSH key identity type such as RSA or DSA. For more information, see SSH Key Profiles on page 433..
Key Length	The supported RSA or DSA key length displays.
Asset Name	Name of the asset associated with the account.
Account	The name of the account where the SSH key was discovered.
Date/Time Discovered	The date and time when the SSH key was discovered.

Use these buttons on the details toolbar.

Table 87: Accounts: Discovered SSH Keys tab toolbar

Option	Description
▶ **Discover SSH Keys**	Run the selected SSH Key Discovery job. A **Task** pop-up display which shows the progress and completion. The button is enabled when the configuration is complete, including a profile (which has a schedule). For more information, see SSH Key Profiles tab (partitions) on page 355..
⊘ **Revoke**	Use this button to revoke access for unmanaged SSH keys.
↻ **Refresh**	Update the list of dependent assets assigned to the selected account.
🔍 **Search**	To locate a specific dependent asset in this list, enter the character string to be used to search for a match. For more information, see For more information, see Search box on page 78..

History tab (account)

The **History** tab allows you to view or export the details of each operation that has affected the selected account.

To access **History**:

- web client: Navigate to **Asset Management** > **Accounts** > (View Details) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
  - **Refresh**: Update the list displayed.
  - **Search**: For more information, see Search box on page 78.

Table 88: Accounts: History tab properties

Property	Description
Date/Time	The date and time of the event.
User	The display name of the user that triggered the event.
Source IP	The network DNS name or IP address of the managed system that triggered the event.
Object Name	The name of the selected account.
Event	The type of operation made to the selected account: • Create • Delete • Update • Add Membership • Remove Membership NOTE: A membership operation indicates a relationship change with a related or parent object such as the selected account was added or removed from the membership of an account group.
Related Object	The name of the related object.
Related Object Type	The type of the related object.

Property	Description
Parent	The name of the object to which the selected account is a child.
Parent Object Type	The parent object type.

Managing accounts

Use the controls and tabbed pages on the Accounts page to perform the following tasks to manage SPP accounts:

- Adding an account
- Adding a cloud platform account
- Manually adding a tag to an account
- Deleting an account
- Adding users or user groups to an account
- Checking, changing, or setting an account password
- Viewing password archive
- Checking, changing, or setting an SSH key
- Viewing SSH key archive
- Checking, changing, or setting an API key
- Viewing API Key Archive

Adding an account

It is the responsibility of the Asset Administrator to add assets and accounts to SPP. While an asset can have multiple accounts, you can only associate an account with one asset.

The new account displays on the **Accounts** list.

NOTE: SPP allows you to set up account discovery jobs that run automatically. For more information, see Account Discovery job workflow on page 384.

To add an account

1. Navigate to **Asset Management** > **Accounts**.
2. Click **+ New Account** from the toolbar.
3. In the **Select the asset for the new account** dialog, select an asset to associate with this account then click **Select Asset**.
4. In the **New Account** dialog, enter the following information:

- On the **General** tab:
  - **Name**:
    - Local account: Enter the login user name for this account. Limit: 100 characters.
    - Directory Account: **Browse** to find the account.
  - **Description**: (Optional) Enter information about this managed account. Limit: 255 characters.
- On the **Management** tab:
  - **Enable Password Request**: This check box is selected by default, indicating that password release requests are enabled for this account. Clear this option to prevent someone from requesting the password for this account. By default, a user can request the password for any account in the scope of the entitlements in which they are an authorized user.

    IMPORTANT: (Azure AD only) Once you save an Azure AD account in SPP you can no longer change the **Application Account** status.
  - **Enable Session Request**: This check box is selected by default, indicating that session access requests are enabled for this account. Clear this option to prevent someone from requesting session access using this account. By default, a user can make an access request for any account in the scope of the entitlements in which they are an authorized user.
  - **Enable SSH Key Request**: This check box is selected by default, indicating that SSH key release requests are enabled for this account. Clear this option to prevent someone from requesting the SSH key for this account. By default, a user can request the SSH key for any account in the scope of the entitlements in which they are an authorized user.
  - **Enable API Key Request**: This check box is selected by default, indicating that API key release requests are enabled for this account. Clear this option to prevent someone from requesting the API key for this account. By default, a user can request the API key for any account in the scope of the entitlements in which they are an authorized user.
  - (Azure AD only) **Application Account**: Within Azure AD, only application accounts can use API keys. In order to select the **Enable API Key Request** check box, this option must be selected for Azure AD accounts which in turn will automatically disallow the use of the **Enable Password Request** option.

    IMPORTANT: Once you save an Azure AD account in SPP you can no longer change the **Application Account** status.
  - **Password Profile** and **SSH Key Profile**: **Browse** to select and assign a profile to govern this account.

    By default an account inherits the profile of its associated asset, but you can assign it to a different profile for this partition. For more information,

see Assigning assets or accounts to a password profile and SSH key profile.

- **Available for use across all partitions** (Only available for some types of directory accounts): When selected, any partition can use this account and the password is given to other administrators. For example, this account can be used as a dependent account or a service account for other assets. Potentially, you may have assets that are running services as the account, and you can update those assets when the service account changes. If not selected, partition owners and other partitions will not know the account exists. Although archive servers are not bound by partitions, this option must be selected for the directory account for the archive server to be configured with the directory account.

5. Click **OK**.

Adding a cloud platform account

One Identity Safeguard for Privileged Passwords can manage cloud platform accounts such as Amazon Web Services (AWS).

Before you add cloud platform accounts to SPP, you must first add an asset with which to associate the accounts. For more information, see Preparing Amazon Web Services platforms.

To add a cloud platform account

1. Navigate to **Asset Management** > **Assets**.
2. Click **+ New Asset** from the toolbar.
3. In the **General** tab:
   a. **Name**: Enter an asset name that is meaningful to you, such as "Cloud Account Server" which you can use to manage all cloud platform accounts.
   b. (Optional) **Description**: Enter a description for the asset.
4. In the **Connection** tab:
   a. **Platform**: Select the appropriate product, such as **Amazon Web Services**.
   b. **Version**: For **Amazon Web Services**, select the version.
   c. **Architecture**: Enter the product's system architecture.
   d. **Network Address**: For **Amazon Web Services**, enter the AWS Account ID or Alias which can be found on the AWS IAM User's view.
   e. **Authentication type**: Select one of the following:
      i. **Access Key** to authenticate to the asset using an access key. Enter the following information:
         - **Service Account Name**: Enter the configured IAM service account.

- **Access Key ID**: Enter the Access Key ID created for the IAM service account.
- **Secret Key**: Enter the Secret Key created for the IAM service account.

ii. **None** to not authenticate to the asset and manually manage the asset.

5. Click **OK** to save.

Once you add the cloud platform asset, you can associate accounts with it.

To add an account to the cloud platform

1. In **Assets**, select the cloud platform asset and switch to the **Accounts** tab.
2. Click **+ New Account** from the details toolbar.
3. In the **Name** field on the **General** tab, enter the cloud platform account username, email address, or phone number.
4. (Optional) Enter a **Description**.
5. On the **Management** tab, ensure the **Enable Password Request** option is checked.
6. Click **Browse** to select a profile to govern this account.
7. Click **Add Account**.
8. Click **OK** to save.

Now you can manually check, change, or set the cloud platform account password; and, SPP can automatically manage the password according to the Check and Change settings in the profile governing the account.

To check out the cloud platform account

1. Add a cloud platform Account Group and add the accounts to the group.
2. Add an entitlement for the cloud platform accounts.
3. Add users to the entitlements.
4. Add a password release policy to the entitlement.
5. Add the cloud platform Account Group to the scope of the policy.

Manually adding a tag to an account

Asset Administrators can manually add and remove static tags to an account. You cannot manually remove dynamically assigned tags which are defined by rules and indicated by a lightening bolt icon. You must modify the rule associated with the dynamic tag if you want to remove it. For more information, see Modifying an asset or asset account tag on page 457..

To manually add a tag to an account

1. Navigate to **Asset Management** > **Accounts**.
2. Select an account and click ✎ **View Details**.
3. Under **Tags**, click **Edit**. Existing tags are displayed.
4. Click ✎ **Edit**.
5. Use one of the following methods to assign tags to the account:
   - To assign a previously created tag:
     1. Click **+ Add Tag**.
     2. Select the tag(s) to add to the account.
     3. Click **Select Tags** to save your selection.
   - To create a new tag:
     1. Click **+ Add Tag**.
     2. From the **Select Tags** dialog, click **+ New Tag**.
     3. Enter the requested information for the tag and click **OK**.
     4. Once finished adding any new tags, select the tag(s) to add to the account on the **Select Tags** dialog.
     5. Click **Select Tags** to save your selection.
6. Click **OK**.

Deleting an account

When you delete an account, SPP does not delete it from its associated asset; it simply removes it from SPP.

If you delete a service account, SPP changes the asset's authentication type to **None**, which disables automatic password and SSH key management for all accounts that are associated with this asset. All assets must have a service account in order to check and change the passwords or SSH keys for the accounts associated with it. For more information, see About service accounts on page 321..

To delete an account

1. Navigate to **Asset Management** > **Accounts**.
2. Select the account to be deleted.
3. Click 🗑 **Delete**.
4. Confirm your request.

Adding users or user groups to an account

When you add users to an account, you are specifying the users or user groups that have ownership of an account.

It is the responsibility of the Asset Administrator (or delegated partition owner) to add users and user groups to accounts. The Security Policy Administrator only has permission to add groups, not users. For more information, see Administrator permissions on page 604..

To add users to an account

1. Navigate to **Asset Management** > **Accounts**.
2. In **Accounts**, select an account from the object list and click **View Details**.
3. Open the **Owners** tab.
4. Click **+ Add** on the Account Owners, Asset Owners, and/or Partition Owners tabs.
5. Select one or more users or user groups from the list in the **Users/User Groups** dialog.
6. Click **Select Owners** to save your selection.

Checking, changing, or setting an account password

The Asset Administrator can manually check, change, or set an account password.

To manually check, change, or set an account password

1. Navigate to **Asset Management** > **Accounts**.
2. In **Accounts**, select an account from the object list.
3. Click (View Details) from the toolbar.
4. Navigate to **Properties** > **Secrets**.
5. The **Password** tile available on this page provides the following options:
    - **Set** to set the account password in the SPP database. The **Set** option does not change the account password on the asset. The **Set** option provides the following options.
        - Manual Password: Use this option to manually set the account password in the SPP database.
            1. In the **Set Password** dialog, enter and confirm the password. Click **Set Password** to update the SPP database.
            2. Set the account password on the physical device to synchronize it with the SPP database.

- Generate Password: Use this option to have SPP generate a new random password, that complies with the password rule that is set in the account's profile.

    1. In the **Set Password** dialog, click **Generate Password**.
    2. Click **Copy Password** to put it into your copy buffer.
    3. Log in to your device (using the old password), and change it to the password in your copy buffer.
    4. Click **Set Password** to change the password in the SPP database.

- **Check** to verify the account password is in sync with the SPP database. If the password verification fails, you can change it.
- **Change** to reset and synchronize the account password with the SPP database.

Viewing password archive

The Asset Administrator can access a previous password for an account for a specific date.

The **Password Archive** dialog only displays previously assigned passwords for the selected asset based on the date specified. This dialog does not display the current password for the asset. The password archive is never purged.

You view an account's password validation and reset history on the **Check and Change Log** tab.

To access an account's previous password

1. Navigate to **Asset Management** > **Accounts**.
2. Select an account and click (View Details).
3. Navigate to **Properties** > **Secrets**.
4. On the **Password** tile, click **View Archive**.
5. In the **Password Archive** dialog, select a date. If you select today's date (or a previous date) and no entries are returned, this indicates that the asset is still using the current password.
6. In the **View** column, click to display the password that was assigned to the asset at that given date and time.
7. In the details dialog, click **Copy** to copy the password to your copy buffer.

Checking, changing, or setting an SSH key

The Asset Administrator can manually check, change, or set an SSH key.

To manually check, change, or set an SSH key

1. Navigate to **Asset Management** > **Accounts**.
2. In **Accounts**, select an account from the object list.
3. Click ✎ **View Details** from the toolbar.
4. Navigate to **Properties** > **Secrets**.
5. The **SSH Key** tile available on this page provides the following options:
6. Select one of these option.
    - **Set** to set the SSH key in the SPP database. The **Set** option does not change the account SSH key on the asset. The **Set** option provides the following options.
        - **Generate an SSH Key**: Generate a new SSH key and assign it to the account. The SSH key complies with the SSH key rule that is set in the account's profile.

          ⚠ **CAUTION: Do not generate a new SSH key for a service account because the connection to the asset will be lost. Instead, use the Change option for SSH Keys.**

          After you select **Generate**, the key is generated and saved in the SPP database. The following fields display.
            - **Account**: The account name
            - **Fingerprint**: The fingerprint of the SSH key used for authentication
            - **Key Comment**: Information about the SSH key
            - **Type**: The SSH authentication key type, such as RSA or DSA. For more information, see SSH Key Profiles on page 433..
            - **Length**: The length of the SSH authentication key. For more information, see SSH Key Profiles on page 433..
            - **Public Key**: The generated key; click **Copy** to put it into your copy buffer. You can then log in to your device, using the old SSH key, and change it to the SSH key in your copy buffer.
        - **Import an SSH Key**: Import a private key file for an SSH key that has been generated outside of SPP and assign it to the account. Click **Browse** to import the key file, enter a **Password**, then click **OK**.

          When importing an SSH key that has already been manually configured for an account on an asset, it is recommended that you first verify that the key has been correctly configured before importing the key. For example, you can run an SSH client program to check that the private key can be used to login to the asset: `ssh -i <privatekeyfile> -l <accountname> <assetIp>`. Refer to the OpenSSH server documentation for the target platform for more details on how to configure an authorized key.

NOTE: SPP does not currently manage the options for an authorized key. If an imported key has any options configured in the authorized keys file on the asset, these options will not be preserved when the key is rotated by SPP.

- **Deploy SSH Key**: If not already configured, install the account's current SSH key on the asset in the correct file for the account.

- **Check** to verify the account SSH key is in sync with the SPP database. If the SSH key verification fails, you can change it.
- **Change** to reset and synchronize the SSH key with the SPP database. For service accounts, use this selection and do not use **Generate SSH Key** to change the SSH key.

Viewing SSH key archive

The Asset Administrator can access a previous SSH key for an account for a specific date.

The **SSH Key Archive** dialog only displays previously assigned SSH keys for the selected asset based on the date specified. This dialog does not display the current SSH key for the asset. The SSH key archive is never purged.

You view an account's SSH key validation and reset history on the **Check and Change Log** tab.

To access an account's previous SSH key

1. Navigate to **Asset Management** > **Accounts**.
2. Select an account and click (View Details).
3. Navigate to **Properties** > **Secrets**.
4. On the **SSH Key** tile, click **View Archive**.
5. In the **SSH Key Archive** dialog, select a date. If you select today's date (or a previous date) and no entries are returned, this indicates that the asset is still using the current SSH key.
6. In the **View** column, click to display the SSH key that was assigned to the asset at that given date and time.
7. In the details dialog, click **Copy** to copy the SSH key to your copy buffer, or click **OK** to close the dialog.

Adding an API key

The Asset Administrator can manually add an API key to an account.

To add an API key

1. Navigate to **Asset Management** > **Accounts**.
2. In **Accounts**, select an account from the object list.
3. Click (View Details) from the toolbar.
4. Navigate to **Properties** > **Secrets**.
5. In the API Keys section, click the **New API Key** button.
6. Depending on the type of account, the following information may be required:
   a. **Name**: Enter the name of the API key. This must match the name used in the platform.
   b. **Description**: Enter a description of the API key.
   c. **Expires**: Enter the number of days before the key will expire.
7. You can also set the API Key to match an existing key for the account. This option does not change the API key information on the platform. This can be done at a later time (using the **Set** button associated with the API key tile) or a new key will be generated when the key is changed. The following options may appear depending on the type of platform:
   a. **Client Identifier**: Copy the client identifier from the platform and add it to this field.
   b. **Client Secret**: Copy the client secret from the platform and add it to the field. Once configured, click **Copy** to put it into your copy buffer. You can then log in to your device, using the old client secret, and change it to the client secret in your copy buffer.
   c. **Client Secret Identifier** (Azure AD only): Copy the client secret identifier from the platform and add it to the field. If the identifier doesn't match, when you attempt to change the API key for the Azure AD platform it will create a new one with the identifier set in Safeguard for SPP.
8. Click **Save**.

Checking, changing, or setting an API key

The Asset Administrator can manually check, change, or set an API key associated with Azure AD and AWS connectors.

To manually check, change, or set an API key

NOTE: Should 4 or more API keys be configured, the tiles will be condensed into a single summary tile. To access and manage the individual API keys, click the name of the tile (**API Keys <*n*>**). This will open a pane containing a table view of the configured API keys as well as toolbar options for managing the keys.

1. Navigate to **Asset Management** > **Accounts**.
2. In **Accounts**, select an account from the object list.

3. Click (View Details) from the toolbar.
4. Navigate to **Properties** > **Secrets**.
5. Each configured API key is represented by a tile available on this page which provides the following options:
    a. **Set** to set the API key secret in the SPP database. This option does not change the API key information on the platform. The following options may appear depending on the type of platform:
        i. **Client Identifier**: Copy the client identifier from the platform and add it to this field.
        ii. **Client Secret**: Copy the client secret from the platform and add it to the field. Once configured, click **Copy** to put it into your copy buffer. You can then log in to your device, using the old client secret, and change it to the client secret in your copy buffer.
        iii. **Client Secret Identifier** (Azure AD only): Copy the client secret identifier from the platform and add it to the field. If the identifier doesn't match, when you attempt to change the API key for the Azure AD platform it will create a new one with the identifier set in Safeguard for SPP.
        iv. **Set Client Secret**: Click this button to save the configuration.
    b. **Check** to verify the API key is in sync with the SPP database. If the API key verification fails, you can change it.
    c. **Change** to reset and synchronize the API key with the SPP database.
    d. (Remove): Click this button to remove a previously configured API Key.

Viewing API Key Archive

The Asset Administrator can access an archive of an account's API Keys.

To access an account's API key archive

1. Navigate to **Asset Management** > **Accounts**.
2. Select an account and click (View Details).
3. Navigate to **Properties** > **Secrets**.
4. For a configured API key, click **View Archive**.
5. In the **API Key archive** dialog, select a date. If you select today's date (or a previous date) and no entries are returned, this indicates that the asset is still using the current API key.
6. In the **View** column, click to display the API Key that was assigned to the asset at that given date and time.
7. In the details dialog, click **Copy** to copy the API Key to your copy buffer.

Setting a TOTP authenticator

Many asset types support the use of a TOTP authenticator for the accounts associated with it using password requests. The following instructions explain how to add a TOTP authenticator to an existing asset.

To set up a TOTP authenticator

1. Navigate to **Asset Management** > **Accounts**.
2. In **Accounts**, select an account from the object list.
3. Click (View Details) from the toolbar.
4. Navigate to **Properties** > **Secrets**.
5. On the **TOTP Authenticator** tile available on this page, click **Set**.
6. On the **Set TOTP Authenticator** pane, select one of the following options:

   NOTE: Once you start the process for setting up a TOTP authenticator you will need to connect the authenticator with the account in SPP by entering the code(s) sent by the authenticator within a set time limit. It is strongly suggested you have your authenticator ready prior to beginning this process to avoid having to restart the setup process due to timing out.

   a. **QR Code Image**: Select this method to connect with the TOTP authenticator through the use of a QR code image file. Click **Browse Your Computer** to select the QR code image file or drag the QR code image file into the dashed box.

   b. **URI or Secret String**: Select this option to connect with the TOTP authenticator through the use of the URI string or secret generated by the authenticator. If only a secret is provided, then the process for generating the string will depend upon the authenticator itself.

      Click **Submit**.
7. A **Setup Confirmation Code** section will appear as soon as the authenticator setup begins and you will need to start entering the provided code(s) into your authenticator (you can use the **Copy** button to copy the code instead of typing the value). The amount of time you have left before the code becomes invalid and a new code is displayed to the right of the **Copy** button.

   The number of code(s) required depends upon the requirements for the authenticator (for example, AWS requires 2 successive codes be entered, with each code being available for approximately 30 seconds. Only 5 codes will be displayed before the authenticator setup times out and you will need to restart the process.). If you are unable to successfully complete the setup, click **Remove Authenticator** to restart the process.
8. Once you have successfully completed the TOTP authenticator setup, click **Done**.

Removing a TOTP authenticator

The following instructions explain how to remove a previously configured TOTP authenticator.

To remove a TOTP authenticator

1. Navigate to **Asset Management** > **Accounts**.
2. In **Accounts**, select an account from the object list.
3. Click (View Details) from the toolbar.
4. Navigate to **Properties** > **Secrets**.
5. On the **TOTP Authenticator** tile available on this page, click **Remove**.
6. On the **Remove Authenticator** confirmation dialog, click **Remove**.

   The previously configured TOTP authentication will no longer be available for the account.

Assets

A SPP asset is a computer, server, network device, or application managed by a SPP Appliance.

It is the responsibility of the Asset Administrator (or delegated partition owner) to add assets and accounts to SPP. The Auditor has permission to access **Assets**. Account owners also have read permissions for the Properties and Accounts tabs for the assets associated with their account.

Before adding assets to SPP, you must ensure they are properly configured. For more information, see Preparing systems for management on page 609.

Each asset can have associated accounts (user, group, and service) identified on the Accounts tab (asset). If an asset is deleted, associated accounts are deleted.

All assets must be governed by a profile (for more information, see Assigning a profile to an asset). All new assets are automatically governed by the default profile unless otherwise specified.

An asset can only be in one partition at a time (for more information, see Assigning an asset to a partition). When you add an asset to a partition, all accounts associated with that asset are automatically added to that partition.

You can identify a default partition and default profile so that when you add assets, the assets are added to the default partition and default profile. For more information, see Setting a default partition on page 362.

Asset Discovery jobs run automatically against the directories you have added. For information about configuring asset discovery in SPP, see Asset Discovery job workflow.

Using a domain controller (DC) asset

You can manage tasks and services on a domain controller (DC) asset. Dependent accounts are managed on the DC asset. A DC asset will only support updating dependent passwords. Account passwords for a domain controller are managed via the directory asset.

1. Create the DC asset as windows server platform, using a directory authentication for the connection service account. For more information, see Adding an asset.
2. Ensure that the service account for the task/service you want to manage is defined in the Directory asset. For more information, see Adding an account to an asset on page 338.
3. Add an account dependency for the service account to the DC asset. For more information, see Adding account dependencies on page 340.

Using Check Point GAiA

In addition to managing user accounts on the Check Point GAiA platform, SPP can also manage the password for the Check Point **expert** command. The **expert** password appears as a normal user account in SPP except that it is marked as a privileged account. This means that it cannot be used as a service account and you cannot generate or install an SSH key for the account.

The minimum requirements for choosing a service account for Check Point follow:

- The service account for Check Point must have CLI access enabled and must have the following RBA features enabled:
  - read-write user
  - read-only group
- In order to manage the expert password, the service account must also have the following RBA features enabled:
  - read-write expert-password-hash
  - read-write expert

To manage SSH keys, the service account must have a Unix shell configured as the login shell. If the UID is not 0, then sudo privileges will be required to elevate privileges.

Managing the enable password for Cisco IOS and ASA

In addition to managing user accounts, Safeguard can also manage the password for the Cisco **enable** command on Cisco IOS and ASA. The enable account appears as a normal user account in Safeguard, except that it is marked as a privileged account. This means that it cannot be used as a service account, and you cannot generate or install an SSH key for it.

The enable password is not automatically managed by Safeguard; it is only managed if an account named `enable` is created on the asset. Once this account is created, the enable password is removed from the asset connection properties (if configured) and can no longer be configured on the asset connection properties. To stop managing the enable password, remove the enable account from the asset which will restore the enable password to the asset connection information.

Safeguard manages the enable password for the default privilege level 15. Safeguard also provides the option to manage enable passwords for other privilege levels, by creating an account called enable<level> (for example, to manage the password for privilege level 10, create an account called `enable10`).

Assets view

To access **Assets**:

- web client: Navigate to **Asset Management** > **Assets**. If needed, you can use the partition drop-down to select the parent partition of the asset. Select an asset, then click to display additional information and options.

The **Assets** view displays the following information about the selected system. Not all selections will be available for all assets.

- Properties tab (asset): Displays general, management and connection settings for the selected asset.
- Owners tab (asset): Displays information about the users and user groups that are owners of the asset (either assigned from this tab or from the ownership derived from a tag associated with this asset). This tab does not list partition owners that are also effective owners of this asset.
- Accounts tab (asset): Displays the accounts associated with this asset.
- Account Dependencies tab (asset): Windows only: Displays the directory accounts that the selected Windows server depends on to perform services and tasks.
- Discovered Services tab (asset): Displays the details of each discovered service associated with the selected asset.
- Discovered SSH Keys (asset): Displays the SSH keys discovered on the asset.
- History tab (asset): Displays the details of each operation that has affected the selected asset.

Toolbar

Use these toolbar buttons to manage assets:

- **+New Asset**: Add assets to SPP. For more information, see Adding an asset.
- **Delete**: Remove the selected asset.
  When you delete an asset, you also permanently delete all the SPP accounts associated with the asset.For more information, see Deleting an asset on page 341.
- **View Details**: Select an asset then click this button to open additional information and options for the asset.
- **Access Request**: Allows you to enable or disable access request services for the selected asset. Menu options include **Enable Session Request** and **Disable Session Request**.

- **SSH Host Key**: Menu options include:
  - **Discover SSH Host Key**: This option only applies to assets that exchange SSH host keys, such as Unix-based assets and Linux-based assets. Retrieves the latest SSH host key for the selected asset. The **Discover SSH Host Key** dialog also tells you when the SSH host key is up-to-date. If the SSH host key is not discovered on the asset, certain tasks will not be available for accounts associated with the asset, such as Check System, Check Password, and Change Password.
  - **Retrieve SSH Host Key**: This option only applies to Cisco NX-OS assets, and is used to retrieve the latest SSH host key from the platform. The **Retrieve SSH Host Key** dialog also tells you when the SSH host key is up-to-date. If the SSH host key is not retrieved from the asset, sessions will not be available.
  - **Set SSH Host Key**: This option allows you to manually add the host key to an asset in cases where SPP cannot discover the asset automatically (such as for an **Other Directory** asset).
  - **Download SSH Key**: Add the SSH key to the selected asset. For more information, see Downloading a public SSH key on page 344.
- **Test Connection**: Select to verify that SPP can log in to the asset using the current service account credentials. For more information, see Checking an asset's connectivity on page 336.
- **Syncronize Now**: Run the directory addition (incremental) synchronization process by asset and account. The sync is queued by asset by provider and runs one directory sync on that asset at a time. You can run multiple syncs in parallel on different assets. This is the faster type of directory sync because deletions are not synced. A **Tasks** window displays the progress and outcome of the task. You can click **Details** to see more information or click **Stop** to cancel the task. In addition, this process runs through the discovery, if there are discovery rules and configurations set up.The API (`Assets/Synchronize`) can be used to run the deletion (full) sync which includes all deletions, additions, and changes. This sync takes longer (perhaps hours), especially the first time it is run based on your directory setup.
- **Discover Accounts**: Run the associated Account Discovery job. For more information, see Account Discovery on page 381.
- **Link Directory Parent**: This option is only available for assets that are members of or joined to a directory, but not linked (which may occur if the asset was manually added to SPP). Clicking this button will allow you to select the parent to which the asset will be linked.

  If the asset resides in a different partition than the parent directory, the **Available for discovery across all partitions** option must be enabled.
- **Enable-Disable**: Select one of the following:

  Select **Enable** to have SPP manage a disabled asset. Account Discovery jobs find all accounts that match the discovery rule's criteria regardless of whether it has been marked **Enabled** or **Disabled** in the past.

Select ⊘ **Disable** to prevent SPP from managing the selected asset. When you disable an asset, SPP disables it and removes all associated accounts. If you choose to manage the asset later, SPP re-enables all the associated accounts.

- **Show Disabled**: Display the assets that are not managed and are disabled and have no associated accounts. Asset management can be controlled by selecting an asset and selecting **Enable-Disable**.
- **Hide Disabled**: Hide the assets that are not managed and are disabled and have no associated accounts. Asset management can be controlled by selecting an asset and selecting **Enable-Disable**.
- **Import**: Use this button to add assets to One Identity Safeguard for Privileged Passwords using a CSV file. For more information, see Importing objects.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of assets.

Properties tab (asset)

The **Properties** tab lists information about the selected asset.

To access the **Properties** tab, in the web client, navigate to **Asset Management** > **Assets** > **View Details** > **Properties**.

Table 89: Properties tab: General properties

Property	Description
Name	The asset name. Assets that are part of a Directory have this automatically synchronized from the Directory.
Description	Description of the selected asset. Assets that are part of a Directory have this automatically synchronized from the Directory.

Table 90: Properties tab: Connection properties

Property	Description
Platform	The platform of the selected managed system.
Version	If applicable, the system version.
Architecture	If applicable, the operating system architecture.
Network Address	If applicable, the network DNS name or IP address of the managed system. Assets that are part of a Directory have this automatically synchronized from the Directory.

Property	Description
Authentication Type	How the console connects with the managed system. For more information, see Custom Properties.
Login with service account name only	If applicable, selecting this option will allow SPP to login the asset using only the service account name. The domain will not be used.
Telnet Session Port	If connecting to TN3270 or TN5250, the port for connection.
Manage Forest (directory)	If **True**, the whole forest is managed.
Forest Root Domain Name (directory)	The forest root domain for the asset (**Name** on the **General** tab). A domain can be identified for more than one directory asset so that multiple directory assets can be governed the same domain.
Managed Domains	If applicable, the managed domains.
Enable Session Request	If **True**, session access requests are enabled for the asset.
Port	The port used for connection. Default is 22.
RDP Session Port	If applicable, the access port on the target server used for RDP session access requests.
SSH Session Port	If applicable, the access port on the target server used for SSH session access requests.
Telnet Session Port	If connecting to TN3270 or TN5250, the port for connection.
SSH Host Key Fingerprint	The managed system's public host key fingerprint used to authenticate to the asset. When an asset requiring an SSH host key does not have one, **Check Password** will fail. For more information, see Connectivity failures on page 638.
Sync additions every [number] minutes	If applicable, the frequency that Safeguard for Privileged Passwords synchronizes the additions or modifications to objects. The date and time of the **Last Sync**, **Last Failure Sync**, and **Last Success Sync** display. The intervals are directory specific.
Sync deletions every [number] minutes	If applicable, the frequency that Safeguard for Privileged Passwords synchronizes the deletion of objects. The date and time of the **Last Delete Sync**, **Last Failure Delete Sync**, and **Last Success Delete Sync** display. The intervals are directory specific.

Table 91: Properties tab: Management properties

Property	Description
Partition	The name of the partition where the selected asset resides.

Property	Description
Password Profile	The name of the profile that manages the asset's accounts. When a password profile is inherited from the partition this will be indicated by the text `(Inherited)` next to the name of the password profile. When the password profile is explicitly set, a ✕ button will appear that allows you to clear the explicitly set password profile and instead use the password profile that is inherited from the partition. NOTE: All assets must be governed by a profile. All new assets are automatically governed by the default profile unless otherwise specified.
SSH Key Profile	The name of the profile that manages the asset's accounts. When an SSH key profile is inherited from the partition this will be indicated by the text `(Inherited)` next to the name of the SSH key profile. When the SSH key profile is explicitly set, a ✕ button will appear that allows you to clear the explicitly set SSH key profile. Once the cleared profile change is applied, the assigned inherited profile will be displayed. If there is no default SSH key profile designated for the partition, the asset will no longer have an SSH key profile assigned. If there is no SSH key profile explicitly set on the asset, the accounts on that asset will no longer have an SSH key profile assigned. Designating a default SSH key profile for the partition will ensure all assets and accounts in that partition have an inherited SSH key profile. NOTE: All assets must be governed by a profile. All new assets are automatically governed by the default profile unless otherwise specified.
Managed Network	The managed network that is assigned for work load balancing. For more information, see Managed Networks on page 201.
Available for discovery across all partitions	If **True**, this asset is read-access available for Asset Discovery jobs beyond partition boundaries.
Enable Session Request	If **True**, session access requests are enabled for the asset.

Table 92: Properties tab: Account Discovery properties

Property	Description
Account Discovery	Account discovery identifier.
Description	The description of the schedule.
Schedule	The account discovery schedule.
Last Successful Account	The date and time of the last successful account

Property	Description
Discovery	discovery.
Last Failed Account Discovery	The date and time of the last failed account discovery.
Next Account Discovery	The date and time for the next account discovery.
Last Successful Service Discovery	The date and time of the last successful service discovery.
Last Failed Service Discovery	The date and time of the last failed service discovery.
Next Service Discovery	The date and time for the next service discovery.

Tags: Tag assignments for the selected asset. The information listed in the **Tags** tab displays both the dynamic tags assigned to the asset through tagging rules and static tags that were added manually. In addition to viewing tag assignments, Asset Administrators can add and remove statically assigned tags using this tab.

Delete: Click this button to delete the selected asset.

Accounts tab (asset)

An asset's **Accounts** tab displays the accounts associated with this asset.

Click **+New Account** from the details toolbar to associate an account with the selected asset.

To access **Accounts**:

- web client: Navigate to **Asset Management** > **Assets** > (View Details) > **Accounts**.

Table 93: Assets: Accounts tab properties

Property	Description
Name	Name of an account associated with the selected asset. While you can associate an account with only one asset, you can log in to an asset with more than one account.
Domain Name	The domain name for the account and helps to determine the uniqueness of accounts.
Password Profile	The name of the profile that manages the account.
SSH Key Profile	The name of the SSH key profile.
Service Account	A ✔ check in this column indicates that the account is a service account.

Property	Description
Password Request	A ✔ check in this column indicates that password release requests are enabled for the account. Click **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected account.
Session Request	A ✔ check in this column indicates that session access requests are enabled for the account. Click **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected account.
SSH Key Request	A ✔ check in this column indicates that SSH key release requests are enabled for the account. Click **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected account.
Disabled	A ✔ check in this column indicates that the asset is not managed, is disabled, and has no associated accounts.
Password	A ✔ check in this column indicates a password is set for the account. For more information, see Checking, changing, or setting an account password on page 291.
TOTP Authenticator	A ✔ check in this column indicates a TOTP Authenticator is set for the account. For more information, see Setting a TOTP authenticator.
SSH Key	A ✔ check in this column indicates an SSH key is set for the account. For more information, see Checking, changing, or setting an SSH key on page 292.
API Keys	A ✔ check in this column indicates an API key is set for the account. For more information, see Checking, changing, or setting an SSH key on page 292.
Description	Descriptive information entered when the account was added.
Tags	The tags associated with the account

Use these buttons on the details toolbar to manage your asset accounts.

Table 94: Assets: Accounts tab toolbar

Option	Description
+ **New Account**	Add accounts to the selected asset. For more information, see Adding an account to an asset on page 338.

Option	Description
Delete	Remove the selected account from the asset.
View Details	Edit the selected account.
Account Secrets	Menu options include: • **Check Password** • **Change Password** • **Check SSH Key** • **Change SSH Key**
Discover SSH Keys	Run the SSH Key Discovery job associated with the account. For more information, see SSH Key Discovery on page 398.
Access Requests	Select an option to enable or disable access request services for the selected account. Values are derived from whether the platform of the asset indicates it supports any of the following: Password Request, SSH Key Request, Session Request. You can enable or disable Password Request, Session Request, and SSH Key Request, as needed. Service Accounts are created when the Asset is created and by default are not enabled for session or password access. Discovered Accounts are controlled by the Account Discovery template that is used in discovering the accounts. They are a property of the rule template of the Account Discovery job. For more information, see Adding an Account Discovery rule on page 387.
Enable-Disable	Select **Enable** to have SPP manage a disabled asset. Account Discovery jobs find all accounts that match the discovery rule's criteria regardless of whether it has been marked **Enabled** or **Disabled** in the past. Select **Disable** to prevent SPP from managing the selected asset. When you disable an asset, SPP disables it and removes all associated accounts. If you choose to manage the asset later, SPP re-enables all the associated accounts.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of asset accounts.
Search	To locate a specific asset account or set of accounts in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Account Dependencies tab (asset)

The **Account Dependencies** tab displays the directory accounts that the selected Windows server depends on to perform services and tasks. The **Account Dependencies** tab is only applicable for a Windows platform when one or more directories have been added to SPP.

Click **Add Account** from the details toolbar above the grid to associate account dependencies with the selected asset. For more information, see Adding account dependencies on page 340.

To access **Account Dependencies**:

- web client: Navigate to **Asset Management** > **Assets** > (View Details) > **Account Dependencies**.

Table 95: Assets: Account Dependencies tab properties

Property	Description
Name	Name of a directory account.
Directory	The directory in which the account resides.
Domain Name	The forest root domain name for the directory.
Distinguished Name	The distinguished name for a directory account.
Description	Description of the dependent account.

The toolbar includes the following:

Table 96: Assets: Account Dependencies tab toolbar

Option	Description
Add Account	Add an account dependency to the selected asset.
Remove Account	Remove the account dependency from the asset.
Refresh	Update the list of account dependencies.
Search	To locate a specific account dependency in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Access Request Policies (asset)

The **Access Request Policies** tab displays the entitlements and access request policies, including password and SSH key release policies and session request policies, associated with the selected asset. This information is available to users that have both Asset Administrator and Policy Administrator permissions.

To access **Access Request Policies**:

- web client: Navigate to **Asset Management** > **Assets** > (View Details) > **Access Request Policies**.

Table 97: Assets: Access Request Policies tab properties

Property	Description
Entitlement	The name of the access request policy's entitlement.
Access Request Policy	The name of the access request policy that governs the selected account.
Accounts	The number of unique accounts in the account groups that are associated with the access request policy.
# Account Groups	The number of unique account groups in the access request policy.
Account Groups	The names of the account groups that associate the selected account with the policy.
Assets	The number of unique assets in the asset groups that are associated with the access request policy.
# Asset Groups	The number of unique assets groups in the access request policy.
Asset Groups	The names of the asset groups that associate the selected account with the policy.

Use these buttons on the details toolbar to manage the dependent assets.

Table 98: Assets: Access Request Policies tab toolbar

Option	Description
Add to Policy	Add the selected asset to the scope of an access request policy.
Remove Selected	Remove the selected policy.
Refresh	Update the list of access request policies.
Search	To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Owners tab (asset)

The **Owners** tab displays information about the owners associated with the account (and its associated assets). For more information on altering the owners assigned via tags, see Modifying an asset or asset account tag.

To access **Owners**:

- web client: Navigate to **Asset Management** > **Assets** > (View Details) > **Owners**.

The **Owners** tab has two views: **Asset Owners** and **Partition Owners**.

Table 99: Assets: Owners tab properties

Property	Description
Asset Owners	
Type	The type of owner.
Name	The name of the owner.
Provider	The name of the authentication provider.
Direct	This column indicates the ownership of the object was assigned directly rather than through the use of a tag.
Via Tag	This column indicates the ownership of the object was assigned through the use of a tag.
Partition Owners	
Type	The type of user or group.
Name	The name of the user or group.
Provider	The name of the authentication provider.

Use the following buttons on the details toolbar to manage the objects owned by the selected asset.

Table 100: Assets: Owners toolbar

Option	Description
+ Add	Add one or more users or user groups to the selected asset. For more information, see Adding users or user groups to an asset.
− Remove	Remove the selected object from being a manager of the selected asset. You can only remove objects directly assigned to an asset (as opposed to those assigned via the use of a tag).

Option	Description
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of owners/managers.
Search	To locate a specific object in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Discovered SSH Keys (asset)

The **Discovered SSH Keys** tab displays the discovered SSH keys for all the accounts of this asset.

To access **Discovered SSH Keys**:

- web client: Navigate to **Asset Management** > **Assets** > (View Details) > **Discovered SSH Keys**.

Table 101: Assets: Discovered SSH Keys tab properties

Property	Description
Fingerprint	The fingerprint of the SSH key used for authentication.
Account Status	The status of the Safeguard account.
SSH Key Managed	This column will have a check mark indicating the SSH key currently in use on the account.
Comment	Free form comment.
Key Type	SSH key identity type such as RSA or DSA. For more information, see SSH Key Profiles on page 433.
Key Length	The supported RSA or DSA key length displays.
Asset Name	Name of the asset associated with the account.
Account	The name of the account where the SSH key was discovered.
Date/Time Discovered	The date and time when the SSH key was discovered.

Use these buttons on the details toolbar.

Table 102: Assets: Discovered SSH Keys tab toolbar

Option	Description
Revoke	Use this button to revoke access for unmanaged SSH keys.
Refresh	Update the list of dependent assets assigned to the selected account.
Search	To locate a specific dependent asset in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Discovered Services tab (asset)

The **Discovered Services** tab displays information specific to the selected asset and is applicable only to Windows assets.

To access **Discovered Services**:

- web client: Navigate to **Asset Management** > **Assets** > (View Details) > **Discovered Services**.

Use these buttons to manage the discovered services.

Table 103: Discovered Services: Toolbar

Option	Description
Discover Services	Run the selected service discovery job. IMPORTANT: Before running a service discovery job, ensure you have used unique names for the services. Services with identical names but different service types may not be accurately discovered. For example, an account/asset using the name `test1` that appears under both Windows and Windows SSH will only return one discovery result despite there being 2 assets/accounts.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of service discovery jobs.
Search	To locate one or more assets, enter the character string to be used to search for a match. For more information, see Search box on page 78.

The following displays for each discovered service.

Table 104: Assets: Discovered Services tab properties

Property	Description
Account	The account in Safeguard that maps to the discovered account associated with the discovered service or task on the asset. This can be a local account or an Active Directory account.
Domain Name	The domain name of the account if the account is an Active Directory account.
System Name	The asset to which the account is associated.
Account Status	The status of the Safeguard account.
Dependent Account	A ✓ check displays if the account is associated as an account dependency on the asset. The value is blank if the account is not associated as an account dependency of the asset.
Service Type	Type of service discovered. Values may be **Service** or **Task**.
Service Name	The name of the discovered service or task.
Service Enabled	A ✓ check displays if the service or task on the asset is enabled. If there is no check mark, the service or task is disabled.
Discovered Account	The discovered service account name configured.
Date/Time Discovered	The date and time when the service or task was discovered.

History tab (asset)

The **History** tab allows you to view or export the details of each operation that has affected the selected asset.

To access **History**:

- web client: Navigate to **Asset Management** > **Assets** > (View Details) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.

- **Refresh**: Update the list displayed.
- **Search**: For more information, see Search box on page 78.

Table 105: Assets History tab properties

Property	Description
Date/Time	The date and time of the event.
User	The display name of the user that triggered the event.
Source IP	The network DNS name or IP address of the managed system that triggered the event.
Object Name	The name of the selected asset.
Event	The type of operation made to the selected asset: • Create • Delete • Update • Add Membership • Remove Membership NOTE: A membership operation indicates a relationship change with a related or parent object such as an account dependency was added or deleted from the selected asset.
Related Object	The name of the related object.
Related Object Type	The type of the related object.
Parent	The name of the object to which the selected asset is a child.
Parent Object Type	The parent object type.

Managing assets

Use the controls and tabbed pages on the **Assets** page to perform the following tasks to manage SPP assets:

- Adding an asset
- Checking an asset's connectivity
- Assigning an asset to a partition
- Assigning a profile to an asset
- Manually adding a tag to an asset
- Adding an account to an asset

- Adding account dependencies
- Adding users or user groups to an asset
- Deleting an asset
- Downloading a public SSH key

Adding an asset

It is the responsibility of the Asset Administrator to add assets and accounts to SPP.

SPP allows you to set up Asset Discovery jobs that run automatically. For more information, see Asset Discovery job workflow on page 367.

Before you add systems to SPP, make sure they are properly configured. For more information, see Preparing systems for management on page 609.

> NOTE: There are special considerations for adding an MS SQL asset to Safeguard. See KB 261806 for details.

To add an asset

1. Navigate to **Asset Management** > **Assets**.
2. Click **+New Asset** from the toolbar.
3. In the dialog, provide information in each of the tabs:

General tab (add asset)	Where you add general information about the asset.
Custom Properties	Where you add the network address, operating system, and version information.
Management tab (add asset)	Where you add the partition, profile information, and enable session requests.
Account Discovery tab (add asset)	Where you add the Account Discovery job.

Related Topics

Adding an account to an asset

Assigning an asset to a partition

Assigning a profile to an asset

Assigning assets or accounts to a password profile and SSH key profile

General tab (add asset)

Use the General tab to specify general information about the asset.

Table 106: Asset: General properties

Property	Description
Name	(Required) Enter a unique display name for the asset. Limit: 100 characters
Description	(Optional) Enter information about this managed system. Limit: 255 characters

Connection tab (add asset)

On the **Connection** tab, select a platform, an **Authentication Type**, and specify the account credentials. If the asset has a custom platform, the **Custom Properties** elements are displayed (for more information, see Custom platforms). When you create a directory asset, accounts created display as discovered accounts in the Discovered Accounts properties grid. For more information, see Discovered Accounts on page 392.

The settings for an asset are shown below.

Table 107: Asset: Connection properties

Property	Description
Platform	Select an operating system or directory service, for this asset. A custom platform can be selected. For more information, see Custom platforms on page 460. **Generic operating system selections:** SPP allows you to select a generic operating system of **Other**, **Other Managed**, **Other Directory**, or **Linux**. This allows you to add an asset to SPP without designating a specific platform. • **Other**: An asset with an **Other** operating system cannot be managed. You can manually change passwords on accounts associated with an asset with an **Other** operating system. SPP cannot connect to the asset so there is no automatic password or SSH key check and change, test connection, or other activity requiring a connection. • **Other Managed**: SPP stores the password or SSH key and can automatically check and change it per the profile configuration. There is no active connection or service account. The passwords are rotated internally and event notifications are sent when the rotation is complete. Another component or piece of automation can change the password or SSH key or make use of the password or SSH key in configuration files. For example, a listener can pick up the change event via the SPP Application to Application (A2A) service and perform actions, as required.

Property	Description
	• **Other Directory**: Other Directory supports the addition of directory properties at the asset and account levels. This allows for the accounts stored on them to be used in session policy via linked accounts or directory account using the access configuration settings. Since an Other Directory is not actually connected to a directory, it is unable to discover accounts or assets that belong to the actual directory that the Other Directory represents. Therefore, all accounts, assets, and credentials will have to be manually entered in SPP. **CAUTION: Since an Other Directory is not actually connected to a directory, you are responsible for making sure that the Other Directory assets and accounts stay in sync with the actual directory that the Other Directory represents.** **For example, if you change the password in SPP the password will not be set in the actual directory. This will cause the account in SPP to be out of sync with the account in the actual directory. Until manually corrected, you will be unable to use the password.** IMPORTANT: Other Directory requires a one to one relationship between the directory and the domain. If your license is per system, this may result in a large number of licenses being required to fully support your assets. • **Linux**: SPP manages an asset with "Linux" on a best effort basis. **Other** platform details: Any **Other** platform type can be changed to a different platform type. Conversely, any platform type can be changed to **Other**; however, any property values specific to the current platform type will be lost. For example, you may want to change a **Linux** operating system to any type of Linux, such as AIX, HP-UX, or Solaris. Then, the specific platform type can be changed back to **Other**, if needed.
Version	(Optional) Select the operating system version. When adding a Linux or Macintosh OS X system, SPP allows you to choose an **Other** version. Custom platforms do not allow for a version to be selected. SPP does not manage passwords for accounts on domain controllers. Manage accounts on domain controllers through the directory asset that hosts the domain controller. For more

Property	Description
	information, see Adding an account to an asset on page 338.
Architecture	(Optional) The product's system architecture. Custom platforms do not allow for an architecture to be set.
Network Address	If applicable, enter a network DNS name or the IP address used to connect to the managed system over the network. For Amazon Web Services assets, enter the Amazon AWS Account ID or Alias. For Safeguard for Privileged Sessions assets, if you're using both REST and SSH as part of your management protocol they will need to be hosted on the same IP.
Starling Agent ID (only available for Connect for Safeguard Assets platforms)	This is required for all assets that are using the Connect for Safeguard Assets service in Starling. Use the **Browse** button to select an agent registered in the Starling subscription. For more information on installing an agent, see the *Connect for Safeguard Assets User Guide*.
Authentication Type	Select the authentication method to use for the asset.
Domain Name (directory)	The domain for the asset (**Name** on the **General** tab). A domain can be identified for more than one directory asset so that multiple directory assets can be governed the same domain.
NetBios Name (Other Directory only)	The NetBios name of the asset.
Domain Unique Id (Other Directory only)	The unique domain identifier for the asset.
Naming Context (Other Directory only)	The naming context for the asset.
Manage Forest (Only available for some types of directory accounts)	Select if you want to manage the whole forest. Do not select if you want to manage just one domain.
Domain Controllers (Only available for some types of directory accounts)	This value is set for a directory (such as Active Directory). To manage tasks and services on a Windows Domain Controller, you need to add a Windows Asset for the Domain Controller. For Active Directory, instead of having SPP automatically find domain controllers from a DNS and CLDAP ping, you can specify domain controllers.

Property	Description
RDP Session Port	If applicable, specify the access port on the target server to be used for RDP session requests. Default: Port 3389
SSH Session Port	If applicable, specify the access port on the target server to be used for SSH session requests. Default: Port 22
Telnet Session Port	If connecting to TN3270 or TN5250, the port for connection. By default, a telnet server typically listens on port 23.
Sync additions every [number] minutes (directory)	Sync additions (incremental sync) syncs all changes except deletions. This is the faster type of sync. For directory assets, enter or select how often you want to synchronize additions (in minutes). This updates Safeguard for Privileged Passwords with any additions or modifications that have been made to the objects, including group membership and user account attributes mapped to Safeguard for Privileged Passwords. The default is 15 minutes and the range is between 1 and 2147483647 minutes. Directory Sync is enabled by default and can be disabled. For more information, see Global Services.
Sync deletions every [number] minutes (directory)	Sync deletions (full sync) syncs all changes and deletions. This sync takes longer (perhaps hours), especially the first time it is run based on your directory setup. For directory assets, enter or select how often you want Safeguard for Privileged Passwords to synchronize deletions (in minutes). This updates Safeguard for Privileged Passwords with any additions, changes, and deletions that have been made to the objects, including group membership and user account attributes mapped to Safeguard for Privileged Passwords. The default is 15 minutes and the range is between 1 and 1440 minutes. Directory Sync is enabled by default and can be disabled. For more information, see Global Services. You can run the deletion (full) sync on demand using the API `Assets/Synchronize` and `IdentityProviders/Synchronize`.
Privileged Account Name (read-only)	When configuring Cisco IOS, Cisco ASA, or Check Point GAiA assets, this read-only field displays **enable** (Cisco IOS and Cisco ASA) or **expert** (Check Point GAiA).
Account Name	For Safeguard for Privileged Sessions assets, enter the name of

Property	Description
	the service account to be managed. Use the **Reset** button to remove a previously configured account.
Hide Alter User command from verbose log_statement logging	This option to hide Alter User commands is enabled by default for new PostgreSQL assets with log_statement configured starting with SPP 7.1. Customers upgrading to 7.1 that want to enable the option will need to reconfigure any existing PostgreSQL assets with log_statement configured to have a service account with superuser permissions and enable the option.

Table 108: Connection tab: Asset authentication types

Authentication Type	Description
SSH Key	To authenticate to the asset using an SSH authentication key.
Directory Account	To authenticate to the asset using a directory account from an external identity store such as Microsoft Active Directory. NOTE: In order to use this authentication type, you must first add a directory asset and add domain user accounts. For more information, see Accounts on page 273.
Starling Connect	To authenticate to the asset using a connector configured in Starling Connect. NOTE: In order to use this authentication type, you must first register a Starling Connect connector. For more information, see Registered Connectors.
Local System Account	For SQL Server assets, to authenticate to the asset using a local system account, which is a Windows user account on the server that is hosting the SQL database.
Password (local service account)	To authenticate to the asset using a local service account and password.
Account Password	When the function account credentials are not in the custom script, for example, Amazon Web Services. For more information, see Adding a cloud platform account on page 288.
Access Key	For Amazon Web Services assets, to authenticate to the asset using an access key. For more information, see Adding a cloud platform account on page 288.
Custom	No authentication information is taken because the custom parameters or parameters in a customer platform script are used. No accounts associated with the asset are stored. For more information, see Custom platforms on page 460.
None	No authentication information is taken and check/change

Authentication Type	Description
	functions are disabled. No accounts associated with the asset are stored. Safeguard for Privileged Passwords discovers the SSH host key of discovered assets even if you selected **None** as the service account credential type.
Test Connection	Verify that Safeguard can log in to the asset using the service account credentials that you have provided.
Timeout	Enter how long to wait (in seconds) for both the connect and command timeout.

Client ID: For SAP assets, enter the client ID.

Custom Properties

If the **Platform** field on the **Connection** tab identified a custom platform, complete the dialog based on the custom properties of the custom platform script. SPP checks to ensure the values match the type of the property that include a string, boolean, integer, or password (which is called secret in the API scripts). SPP cannot check the validity or system impact of values entered for custom platforms.For more information, see Creating a custom platform script on page 461.

About service accounts

SPP uses a service account to connect to an asset to securely manage accounts and passwords on that asset. Therefore, a service account needs sufficient permissions to edit the passwords of other accounts.

When you add an asset, SPP adds its service account to the list of **Accounts**. By default, SPP automatically manages the service account password and SSH keys according to the check and change schedules in the profile that governs its asset. See: Creating a password profile and Creating an SSH key profile.

When adding a service account, SPP automatically disables it from access requests. If you want the password or SSH key to be available for release, click **Access Requests** and select **Enable Password Request** or **Enable SSH Key Request**. If you want to enable session access, select **Enable Session Request**.

> TIP: As a best practice, if you do not want SPP to manage a service account password or SSH key, add the account to a profile that is set to never change passwords or SSH keys.

If you delete a service account, SPP changes the asset's authentication type to **None**, which disables automatic password or SSH key management for all accounts that are associated with this asset. A user can continue to check out the passwords or SSH keys, however, if the policy that governs the account requires that it change the password or SSH

key after release, the password or SSH key can get stuck in a pending password reset state. For more information, see Password or SSH key is pending a reset on page 645..

Test connectivity

The most common causes of failure in SPP are either connectivity issues between the appliance and the managed system, or problems with service accounts. If you experience issues, first verify that you can access the managed system from another system (independent of SPP), using the service account. For more information about troubleshooting connectivity issues, see Test Connection failures and Connectivity failures.

About Test Connection

When adding an asset, **Test Connection** verifies that SPP can log in to the asset using the service account credentials that you have provided.

When adding an asset that requires an SSH host key, **Test Connection** first discovers the key and presents it to you for acceptance. When you accept it, **Test Connection** then verifies that SPP can log in to the asset using the service account credentials that you have provided.

Once you save the new asset, SPP saves the service account credentials. SPP uses these credentials to connect to an asset to securely manage accounts and passwords on that asset. For more information, see About service accounts on page 321..

If you want to verify an existing asset's connectivity, use the **Test Connection** button in the web client. For more information, see Checking an asset's connectivity on page 336..

If you have entered values for **Specify Domain Controllers** and if SPP does not find a domain controller in the list, the test connection fails and an error is returned.

Related Topics

Test Connection failures

SSH Key

On the Connection tab, you can configure SPP to authenticate to a managed system using an SSH authentication key. To rotate SSH keys, you must select the **Manage SSH Key** option in the asset's profile change schedule. For more information, see Adding SSH key change settings on page 439.

> NOTE: This option is not available for all operating systems. But if a SPP asset requires an SSH host key and does not have one, **Check SSH Key**, **Change SSH Key**, and **Test Connection** will fail. For more information, see Connectivity failures on page 638.

The information that displays depends on whether you choose to automatically generate the SSH key or import and manually deploy the SSH key.

Table 109: SSH Key authentication type properties

Property	Description

SSH Key Generation and Deployment	Select one of the following options:
	• **Automatically generate and deploy a new SSH Key**
	  • In the **Password** field, enter the password for the SSH Key.
	• **Automatically generate a new SSH Key that I will deploy myself**
	• **Import an SSH Key that I will deploy myself**
	  NOTE: SPP does not currently manage the options for an authorized key. If an imported key has any options configured in the authorized keys file on the asset, these options will not be preserved when the key is rotated by SPP.
	  i. Click **Browse**. On the **Import an SSH Key** dialog, click **Browse** then select the Private Key File.
	  ii. Enter a **Password**, if desired. A password is required if the private key is encrypted.
	  iii. Click **Import**.

Key Comment	(Optional) Enter a description of this SSH key. Maximum length of 225 characters.
Account Name	Enter the service account name that SPP is to use for management tasks. This is the account SPP uses to install the SSH authentication key on the asset. For more information, see About service accounts on page 321.
Privilege Elevation Command	If required, enter a privilege elevation command (such as `sudo`). This is used as a prefix for commands that require privileged access on the system and to manage accounts on Unix-based systems; that is, to check and change SSH keys and to discover accounts. Sudo commands follow. • AuthorizedKeyCommand Specify a program to look up the user's public keys • cat • chmod • chown • cp • echo • egrep • find

Property	Description
	• grep • host • ls • mkdir • mv • rm • sed • sshd • ssh-keygen • tee • test • touch • usermod When adding an asset, this command is used to perform **Test Connection**. For more information, see About Test Connection on page 322. The privilege elevation command must run non-interactively, that is, without prompting for a password. For more information, see Preparing Unix-based systems on page 628. The limit is 255 characters.
Auto Accept SSH Host Key	Select this option to have SPP automatically accept the SSH host key when it creates the SPP asset. When this option is selected, SPP displays the thumbprint of the SSH host key that was discovered. When a managed system requiring an SSH host key does not have one, **Check SSH Key** will fail. For more information, see Connectivity failures on page 638.
Test Connection	Click this button to verify that SPP can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 322.
Port	Enter the port number used by SSH to log in to the managed system. Required
Connection Timeout	Enter how long to wait (in seconds) for both the connect and command timeout. Default: 20 seconds
(Custom	If there is a custom parameter in the custom platform script, enter the

Property	Description
platform operation e.g Check System Properties)	custom parameter here. The list of system parameters are here: Writing a custom platform script. Any parameter not in the list is a custom parameter.

Directory Account

NOTE: Only available for some types of directory accounts.

On the Connection tab, you can configure SPP to authenticate to a managed system using an account from an external identity store such as Microsoft Active Directory. In order to use this authentication type, you must first add a directory asset to SPP and add domain user accounts. Managed account users cannot be members of the Protected Users AD Security Group. For more information, see Accounts on page 273.

Table 110: Directory Account authentication type properties

Property	Description
Service Account Name	Click **Select Account**. Choose the service account name used for management tasks. The accounts available for selection are domain user accounts that are linked to a directory that was previously added to SPP.
Service Account Password	If required, enter the password used to authenticate.
Privilege Elevation Command	If required, enter a privilege elevation command (such as `sudo`). This is used as a prefix for commands that require privileged access on the system and to manage accounts on Unix-based systems; that is, to check and change SSH keys and to discover accounts. Sudo commands follow. • AuthorizedKeyCommand Specify a program to look up the user's public keys • cat • chmod • chown • cp • echo • egrep • find

Property	Description
	• grep • host • ls • mkdir • mv • rm • sed • sshd • ssh-keygen • tee • test • touch • usermod When adding an asset, this command is used to perform **Test Connection**. For more information, see About Test Connection on page 322. The privilege elevation command must run non-interactively, that is, without prompting for a password. For more information, see Preparing Unix-based systems on page 628. The limit is 255 characters.
Test Connection	Click this button to verify that SPP can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 322.
Service Account Profile	Click **Edit** to add the profile or **— Remove** to delete the assigned profile. Available profiles are based on the partition selected on the General tab (asset discovery). To update the profile later, go to the service account and update the profile. For more information, see Properties (account) on page 274.
Use Named Pipe for service account connection	Select to use the Named Pipe when connecting to the asset. Clear this check box to use TCP/IP when connecting to the asset.
Use SSL Encryption	Selected by default, this option is used to enable Safeguard to encrypt communication with this asset. To support SSL on Active Directory, you must upload the SSL certificate being used by the Active Directory forest. The SSL binds will need to be on port 636. For information on this

Property	Description
	process within Active Directory, see Enable LDAP over SSL with a third-party certificate authority. If you do not select this option for a MicrosoftSQL Server that is configured to force encryption, **Test Connection** will use untrusted encryption and succeed with valid credentials. For more information about how Safeguard database servers use SSL, see How do SPP database servers use SSL.
Verify SSL Certificate	Use this option to enable or disable SSL Certificate verification on the asset. When enabled, Safeguard for Privileged Passwords compares the signing authority of the certificate presented by the asset to the certificates in the Trusted CA Certificates store every time Safeguard for Privileged Passwords connects to the asset. Trust must be established for Safeguard for Privileged Passwords to manage the asset. For Safeguard for Privileged Passwords to verify an SSL certificate, you must add the asset's signing authority certificate to the Trusted CA Certificates store. Only clear the **Verify SSL Certificate** option if you do not want to establish trust with the asset.
Privilege Level Password	If required, enter the system enable password to allow access to the Cisco configuration.
Auto Accept SSH Host Key	Select this option to have SPP automatically accept an SSH host key. When an asset requiring an SSH host key does not have one, **Check Password** will fail. For more information, see Connectivity failures on page 638.
Instance	Specify the Instance name if you have configured multiple instances of a SQL Server on this asset. If you have configured a default (unnamed) instance of the SQL Server on the host, you need to provide the IP address and port number.
Port	Enter the port number to log in to the asset. This option is not available for all operating systems.
Connection Timeout	Enter the directory connection timeout period. Default: 20 seconds.

Starling Connect

On the Connection tab, you can configure SPP to authenticate to a registered connector in Starling Connect. In order to use this authentication type, you must first register a Starling Connect connector. For more information, see Registered Connectors.

Table 111: Starling Connect authentication type properties

Property	Description
Test Connection	Click this button to verify that SPP can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 322.
Connection Timeout	Enter the directory connection timeout period. Default: 20 seconds.

Local System Account

On the Connection tab, you can configure SPP to authenticate to a managed SQL Server using a local system account and password. The local system account is a Windows user account on the server that is hosting the SQL database.

NOTE: In order to use this authentication type, you must add both a Windows asset and a SQL Server asset to SPP.

Table 112: Local System Account authentication type properties

Property	Description
Test Connection	Click this button to verify that SPP can log in to this asset using the local system account credentials you have provided. For more information, see About Test Connection on page 322.
Use SSL Encryption	Select this option to enable Safeguard to encrypt communication with this asset. If you do not select this option for a MicrosoftSQL Server that is configured to force encryption, **Test Connection** will use untrusted encryption and succeed with valid credentials. For more information about how Safeguard database servers use SSL, see How do SPP database servers use SSL.
Verify SSL Certificate	Use this option to enable or disable SSL Certificate verification on the asset. When enabled, Safeguard for Privileged Passwords compares the signing authority of the certificate presented by the asset to the certificates in the Trusted CA Certificates store every time Safeguard for Privileged Passwords connects to the asset. Trust must be established for Safeguard for Privileged Passwords to manage the asset. For Safeguard for Privileged Passwords to verify an SSL certificate, you must add the asset's signing authority certificate to the Trusted CA Certificates store. Only clear the **Verify SSL Certificate** option if you do not want to establish trust with the asset.
Instance/Service Name	For SQL Server platforms, specify the **Instance** name if you have configured multiple instances of a SQL Server on this

Property	Description
	asset. If you have configured a default (unnamed) instance of the SQL Server on the host, you need to provide the IP address and port number. For Oracle platforms, use the TNSNAMES naming method to identify the target system in Oracle. Depending on how the Oracle environment is configured, the **Instance** (also called SID in Oracle) and/or the **Service Name** (ServiceName) can be used to identify the target database.
Port	Enter the port number to log in to the asset.
Connection Timeout	Enter how long to wait (in seconds) for both the connect and command timeout. Default: 20 seconds

Password (local service account)

On the Connection tab, you can configure SPP to authenticate to a managed system using a local service account and password.

NOTE: Some options are not available for all operating systems.

Table 113: Password authentication type properties

Property	Description
Distinguished Name	For LDAP platforms, enter the fully qualified distinguished name (FQDN) for the service account. For example: `cn=dev-sa,ou=people,dc=example,dc=com`
Service Account Distinguished Name	**Browse** to select the service account for SPP to use for management tasks. When you add the asset, SPP automatically adds the service account to **Accounts**. For more information, see About service accounts on page 321. Required except for LDAP platforms, which use the Distinguished Name.
Password	Enter the service account password used to authenticate to this asset. Limit: 255 character
Privilege Elevation Command	If required, enter a privilege elevation command (such as `sudo`). This is used as a prefix for commands that require privileged access on the system and to manage accounts on Unix-based systems; that is, to check and change SSH keys and to discover accounts. Sudo commands follow.

Property	Description
	• AuthorizedKeyCommand Specify a program to look up the user's public keys • cat • chmod • chown • cp • echo • egrep • find • grep • host • ls • mkdir • mv • rm • sed • sshd • ssh-keygen • tee • test • touch • usermod When adding an asset, this command is used to perform **Test Connection**. For more information, see About Test Connection on page 322. The privilege elevation command must run non-interactively, that is, without prompting for a password. For more information, see Preparing Unix-based systems on page 628. The limit is 255 characters.
Privilege Level Password	Enter the Enable password to allow access to the Cisco configuration.
Auto Accept SSH Host Key	This check box is selected by default indicating that SPP automatically accepts an SSH host key. This option is not available for all platforms.

Property	Description
	Once the SSH host key is discovered, the SSH host key fingerprint is displayed. When an asset requiring an SSH host key does not have one, **Check Password** will fail. For more information, see Connectivity failures on page 638.
Test Connection	Click this button to verify that SPP can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 322.
Service Account Password Profile	Click **Edit** to add the profile or **— Remove** to delete the assigned profile. Available profiles are based on the partition selected on the General tab (asset discovery). To update the profile later, go to the service account and update the profile. For more information, see Properties (account) on page 274.
Service Account SSH Key Profile	Click **Edit** to add the profile or **— Remove** to delete the assigned profile. Available profiles are based on the partition selected on the General tab (asset discovery). To update the profile later, go to the service account and update the profile. For more information, see Properties (account) on page 274.
Use SSL Encryption	Select this option to enable Safeguard to encrypt communication with this asset. If you do not select this option for a MicrosoftSQL Server that is configured to force encryption, **Test Connection** will use untrusted encryption and succeed with valid credentials. For more information about how Safeguard database servers use SSL, see How do SPP database servers use SSL
Verify SSL Certificate	Use this option to enable or disable SSL Certificate verification on the asset. When enabled, Safeguard for Privileged Passwords compares the signing authority of the certificate presented by the asset to the certificates in the Trusted CA Certificates store every time Safeguard for Privileged Passwords connects to the asset. Trust must be established for Safeguard for Privileged Passwords to manage the asset. For Safeguard for Privileged Passwords to verify an SSL certificate, you must add the asset's signing authority certificate to the Trusted CA Certificates store. Only clear the **Verify SSL Certificate** option if you do not want to establish trust with the asset.
As Privilege	Specify the Oracle privilege level to use when connecting with the selected Oracle service account, if required. The Oracle SYS account requires the privilege level SYSDBA or SYSOPER. For details, see the Oracle document, About

Property	Description
	Administrative Accounts and Privileges and SYSDBA and SYSOPER System Privileges.
Instance/Service Name	For SQL Server platforms, specify the **Instance** name if you have configured multiple instances of a SQL Server on this asset. If you have configured a default (unnamed) instance of the SQL Server on the host, you need to provide the IP address and port number. For Oracle platforms, use the TNSNAMES naming method to identify the target system in Oracle. Depending on how the Oracle environment is configured, the **Instance** (also called SID in Oracle) and/or the **Service Name** (ServiceName) can be used to identify the target database.
Workstation ID	Specify the configured workstation ID, if applicable. This option is for IBM i systems.
Port	Enter the port number on which the asset will be listening for connections. Default: port 22; port 1433 for SQL server; port 8443 for SonicWALL SMA or CMS appliance.
Connection Timeout	Enter how long to wait (in seconds) for both the connect and command timeout. Default: 20 seconds

Access Key

On the Connection tab, you can configure SPP to authenticate to a managed system using an access key.

Table 114: Access Key authentication type properties

Property	Description
Service Account	Enter an account for SPP to use for management tasks. For more information, see About service accounts on page 321.
Access Key ID	Enter the unique identifier that is associated with the secret key. The access key ID and secret key are used together to sign programmatic AWS requests cryptographically. Limit: 32 alphanumeric characters
Secret Key	Enter a secret access key used to cryptographically sign programmatic Amazon Web Services (AWS) requests. Limit: 40 alphanumeric characters; the + and the / characters are also allowed.

Property	Description
Test Connection	Click this button to verify that SPP can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 322.
Port	Enter the port number to log in to the asset.
Connection Timeout	Enter the connection timeout period. Default: 20 seconds

None

When the asset's **Authentication Type** on the **Connection** tab is set to **None**, SPP does not manage any accounts associated with the asset and does not store asset related credentials.

All assets must have a service account in order to check and change the passwords for the accounts associated with the asset.

Select the **Auto Accept SSH Host Key** to have Safeguard for Privileged Passwords automatically accept the SSH host key when it creates the archive server. For more information, see Adding an archive server on page 153.

You can also use the **SSH Session port** field to specify the access port on the target server to be used for SSH session requests (default is port 22).

Management tab (add asset)

Use the **Asset Management** > **Assets** > **Management** tab to add the partition and profile to which the asset is assigned. An asset can only be in one partition at a time. When you add an asset to a partition, all accounts associated with that asset are automatically added to that partition. All assets must be governed by a profile. New assets are automatically governed by the default profile unless otherwise specified.

The settings for an asset are shown below.

Table 115: Asset: Management tab properties

Property	Description
Partition	**Browse** to select a partition for this asset. You can set a specific partition as the default, see Setting a default partition.
Password Profile	**Browse** to select a password profile to manage this asset's accounts. You must assign all assets to a profile. All new assets are assigned to the default profile unless you specify another. You can set a specific profile as the default. For more information, see Setting a default profile on page 363. Click **Reset** to set the profile to the current default.

Property	Description
	The **Reset** button only becomes active when the asset has been explicitly assigned to the profile. If the asset is only implicitly assigned to the profile, the **Reset** button is not activated. If you do not explicitly assign an asset to a profile, it is always assigned to the current default profile.
SSH Key Profile	**Browse** to select an SSH key profile to manage this asset's accounts. You must assign all assets to a profile. All new assets are assigned to the default profile unless you specify another. You can set a specific profile as the default. For more information, see Setting a default profile on page 363. Click **Reset** to set the profile to the current default. The **Reset** button only becomes active when the asset has been explicitly assigned to the profile. If the asset is only implicitly assigned to the profile, the **Reset** button is not activated. If you do not explicitly assign an asset to a profile, it is always assigned to the current default profile.
Enable Session Request	If applicable, this check box is selected by default, indicating that authorized users can request session access for this asset. Clear this check box if you do not want to allow session requests for this asset. If an asset is disabled for sessions and an account on the asset is enabled for sessions, sessions are not available because the asset does not allow sessions.
Available for discovery across all partitions	Available for LDAP, Red Hat Directory Server and eDirectory LDAP assets; select this check box to allow the asset to be discovered across all partitions.
Manage using hashed password	Available for LDAP, Red Hat Directory Server and eDirectory LDAP assets; selecting this check box indicates password encryption will be performed by Safeguard when performing a Change Password operation.
Managed Network	The managed network that is assigned for work load balancing. For more information, see Managed Networks on page 201.

Attributes tab (edit asset)

NOTE: The **Attributes** tab only appears after you have successfully added a new asset and is accessed by editing the asset.

In the web client, the Attributes tab is used to add attributes to directory assets (including Active Directory and LDAP). For more information, see Adding identity and authentication providers.

IMPORTANT: Some Active Directory attributes are fixed and cannot be changed.

Table 116: Active Directory and LDAP: Attributes tab

SPP Attribute	Directory Attribute
User	
ObjectClass	Default: `user` for Active Directory, `inetOrgPerson` for LDAP Click **Browse** to select a class definition that defines the valid attributes for the user object class.
Username	`sAMAccountName` for Active Directory, `cn` for LDAP
Password	`userPassword` for LDAP
Description	`description`
MemberOf	Blank by default, this attribute can be set to a directory schema attribute that contains the list of directory groups of which the user is a member.
Alternate Login Name	`userPrincipalName` NOTE: By default the Alternate Login Name attribute for directories is set to `userPrincipalName`, however another directory attribute containing a UPN type account name can be used. This attribute can be used in conjunction with the API's `UseAltLoginName` setting (disabled by default) which will instead use the Alternate Login Name as the account name. The API is PUT https://<host>/service/core/v4/AccessPolicies/{id} where the {id} is the id of the `accessPolicy` where you'll set the `UseAltLoginName` to true. `UseAltLoginName` is a boolean field on the asset data object.
Group	
ObjectClass	Default: `group` for Active Directory, `groupOfNames` for LDAP Click **Browse** to select a class definition that defines the valid attributes for the computer object class.
Name	`sAMAccountName` for Active Directory, `cn` for LDAP
Member	`member`
Computer	
ObjectClass	Default: `computer` for Active Directory, `ipHost` for LDAP Click **Browse** to select a class definition that defines the valid attributes for the computer object class.
Name	`cn`
Network Address	`dNSHostName` for Active Directory, `ipHostNumber` for LDAP

SPP Attribute	Directory Attribute
Operating System	`operatingSystem` for Active Directory
Operating System Version	`operatingSystemVersion` for Active Directory
Description	`description`

Checking an asset's connectivity

After you add an asset you can verify that SPP can log in to it using the **Test Connection** option.

NOTE: When you run **Test Connection** from the asset's **Connection** tab (such as when you add the asset initially), you must enter the service account credentials. Once you add the asset to SPP it saves these credentials.

The **Test Connection** option does not require that you enter the service account credentials because it uses the saved credentials to verify that it can log in to that asset.

To check an asset's connectivity

1. Navigate to **Asset Management** > **Assets**.
2. Select an asset.
3. Click the **Test Connection** button.

   SPP displays a task pane that shows the results.

Assigning an asset to a partition

Use the **Assets** view to assign an asset to a partition. An asset can only be in one partition at a time. When you add an asset to a partition, all accounts associated with that asset are automatically added to that partition, as well.

You cannot remove an asset from a partition. However, you can add the asset to another partition either from the scope of the other partition or from an asset's **Properties** tab.

To assign an asset to a partition

1. Navigate to **Asset Management** > **Assets**.
2. Select an asset and click **View Details**.
3. Under **Management**, click **Edit**.
4. Click the **Browse** button associated with the **Partition** field.
5. Once you have selected a partition, click **Select Partition** to save the selection.
6. Click **OK** to save your changes.

Assigning a profile to an asset

Use the **Assets** view to assign a profile to an asset.

To assign a profile to an asset

1. Navigate to **Asset Management** > **Assets**.
2. Select an asset and click **View Details**.
3. Under **Management**, click **Edit**.
4. Click the **Browse** button associated with the **Password Profile** field.
5. Once you have selected a password profile, click **Select Password Profile** to save the selection. You can only choose profiles that are in the selected asset's partition.
6. Click **OK** to save your changes.

Manually adding a tag to an asset

Asset Administrators can manually add and remove static tags to an asset using the **Tags** pane, which is located at the bottom of the **General** tab when an asset is selected on the **Assets** view.

You cannot manually remove dynamically assigned tags which are defined by rules and indicated by a lightening bolt icon. You must modify the rule associated with the dynamic tag if you want to remove it. For more information, see Modifying an asset or asset account tag on page 457.

To manually add a tag to an asset

1. Navigate to **Asset Management** > **Assets**.
2. Select an asset and click **View Details**.
3. Under **Tags**, click **Edit**. Existing tags are displayed.
4. Use one of the following methods to assign tags to the asset:
   - To assign a previously created tag:
     a. Click **Add Tag**.
     b. In the **Select Tags** dialog, select the tag(s) to add to the asset.
     c. Click **Select Tags** to save your selection.
   - To create a new tag:
     a. Click **Add Tag**.
     b. In the **Select Tags** dialog, click **New Tag**.

c. Enter the requested information for the tag and click **OK**.

d. Once finished adding any new tags, select the tag(s) to add to the asset.

e. Click **Select Tags** to save your selection.

5. Click **OK**.

Adding an account to an asset

Use the **Accounts** tab on the **Assets** view to add an account to an asset.

You can manage tasks and services on a domain controller (DC) asset. For more information, see Using a domain controller (DC) asset on page 299.

You can add an account to an asset or add a directory account to a directory asset. Steps for both follow.

To add an account to an asset

1. Navigate to **Asset Management** > **Assets**.
2. Select an asset and click **View Details**.
3. Open the **Accounts** tab.
4. Click **+ New Account** from the details toolbar.
5. On the General tab, enter the following information:
   - **Name**:
     - Local account: Enter the login user name for this account. Limit: 100 characters.
     - Directory Account: **Browse** to find the account.
   - **Description**: (Optional) Enter information about this managed account. Limit: 255 characters.
6. On the Management tab, enter the following information:
   - **Enable Password Request**: This check box is selected by default, indicating that password release requests are enabled for this account. Clear this option to prevent someone from requesting the password for this account. By default, a user can request the password for any account in the scope of the entitlements in which they are an authorized user.
   - **Enable Session Request**: This check box is selected by default, indicating that session access requests are enabled for this account. Clear this option to prevent someone from requesting session access using this account. By default, a user can make an access request for any account in the scope of the entitlements in which they are an authorized user.
   - **Password Profile**: **Browse** to select a profile to govern this account.

     By default an account inherits the profile of its associated asset, but you can assign it to a different profile for this partition. For more information, see

Assigning assets or accounts to a password profile and SSH key profile on page 363.

- **Available for use across all partitions** (For directory accounts only): When selected, any partition can use this account and the password is given to other administrators. For example, this account can be used as a dependent account or a service account for other assets. Potentially, you may have assets that are running services as the account, and you can update those assets when the service account changes. If not selected, partition owners and other partitions will not know the account exists. Although archive servers are not bound by partitions, this option must be selected for the directory account for the archive server to be configured with the directory account.

7. Click **OK** to save the account to the asset..

Directory assets

If you add directory user accounts to a directory asset, Safeguard for Privileged Passwords will automatically change the user passwords according to the profile schedule you set, which could prevent a directory user from logging into Safeguard for Privileged Passwords. For information about how to set up directory users as Safeguard for Privileged Passwords users, see Adding a user.

For Active Directory, the standard global catalog port, 3268 (LDAP), must be open on the firewall for every Windows global catalog server in the environment and SPP Appliance to communicate for directory management tasks (for example, adding a directory account, a directory user account, or a directory user group). LDAP uses port 389 for unencrypted connections. For more information, see the Microsoft publication How the Global Catalog Works.

To add a directory account to a directory asset

1. Navigate to **Asset Management** > **Assets**.
2. Select a directory asset and click **View Details**.
3. Open the **Accounts** tab.
4. Click **+New Account** from the details toolbar.
5. In the **New Account** dialog, click **Select Account**.
6. In the **Account Search Options** dialog:
   a. **Starts With (Active Directory ANR Search)**: Use this field to enter a full or partial account name.
   b. **Search Location**: Use the **Browse** button to select a container within the directory as the Search Location.
   c. The **Include objects from sub containers** check box is selected by default, indicating that child objects will be included in your search. Clear this check box to exclude child objects from your search.
   d. Click **Find Account** to search for the account.

7. The results of the search displays in the **Select Account** grid. Select an account to add to SPP.
8. To save the selected accounts, click **Select Account**.
9. Click **OK** to save the directory account to the directory asset.

Adding account dependencies

One or more Windows servers can use a directory account (such as an Active Directory account) to run hosted services and/or tasks. The Asset Administrator can configure a dependency relationship between the directory account and the Windows servers. SPP performs dependent system updates to maintain the passwords for dependent accounts on all the systems that use them. For example, when SPP changes the directory account password, it updates the credentials on all the Windows server's dependent accounts so that the services or tasks using this account are not interrupted. Also see KB article 312212.

You can manage tasks and services on a domain controller (DC) asset. For more information, see Using a domain controller (DC) asset on page 299.

Configuring account dependencies on an asset

1. Directory accounts:
   a. You must add directory accounts before you can set up account dependency relationships. For more information, see Adding an account on page 286.
   b. From the directory account, select the **Available for use across all partitions** option so it can be used outside its domain partition. For more information, see Adding an account on page 286.
2. Assets: You must add the target directory account as a dependent account for the asset. The service account can be a domain account (to look up domain information) or a local account if the asset is a Windows Server platform. The service account can be a domain or local account if the asset is a Windows Server platform. If the asset is a Windows SSH platform, then the service account must be a domain account in order to update dependent accounts.

   > IMPORTANT: For Windows SSH assets, a local account does not have the access necessary to discover services running as domain accounts. So if a local account is used, SPP will only discover services running as local accounts, and domain account dependencies will not be updated.

   Follow these steps:

   a. Navigate to:
      - web client: **Asset Management** > **Assets**.
   b. Select the asset (such as a Windows server) from the object list and open the **Account Dependencies** tab.

c. Click + **New Account** from the details toolbar and select one or more directory accounts. SPP only allows you to select directory accounts.

3. Profiles:

   a. The target directory account must be in the same profile as the dependent asset.

   b. You must configure the dependent asset's profile in the **Change Password** tab to perform the required updates on the asset. For example, select the **Update Service on Password Change** check box and so on. For more information, see Creating a password profile on page 361.

Adding users or user groups to an asset

When you add users to an asset, you are specifying the users or user groups that have ownership of an asset.

It is the responsibility of the Asset Administrator (or delegated partition owner) to add users or user groups to assets. The Security Policy Administrator only has permission to add groups, not users. For more information, see Administrator permissions on page 604.

To add users to an account

1. Navigate to **Asset Management** > **Assets**.
2. In **Assets**, select an asset from the object list and click **View Details**.
3. Open the **Owners** tab.
4. Click + **Add**.
5. Select one or more users or user groups from the list in the **Select users and groups** dialog.
6. Click **Select Owners** to save your selection.

Deleting an asset

The Asset Administrator can delete an asset even if there are active access requests.

IMPORTANT: When you delete an asset, you also permanently delete all the SPP accounts associated with the asset.

To delete an asset

1. Navigate to **Asset Management** > **Asset**.
2. Select the asset to be deleted.
3. Click **Delete**.
4. Confirm your request.

Account Discovery tab (add asset)

The **Account Discovery** tab is only available after an Active Directory or Safeguard for Privileged Sessions asset has been created. On the **Account Discovery** tab, the default is `Do not perform account discovery`.

To access **Account Discovery**:

- web client: Navigate to **Asset Management** > **Assets** > **Account Discovery**.

The settings outlined in the following table are available by using the **Add** or **Edit** option available from the **Account Discovery** tab.

Table 117: Account Discovery tab properties

Property	Description
Description	Select the description of the discovery job desired and the details of the configuration display. Click **Add** to add a job or **Edit** to edit the job. You can click the drop-down and select **Do not perform account discovery**.
Partition	The partition in which to manage the discovered assets or accounts.
Discovery Type	The type platform, for example, Windows, Unix, or Directory.
Directory	The directory for account discovery.
Account Discovery Rules	You can click **Add**, **Delete**, **Edit**, or **Copy** to update the Rules grid. Details about the selected account discovery setting rules may include the following based on the type of asset. • **Name**: Name of the discovery job. • **Rule Type**: What the search is based on. For example, the rule may be **Name** based or **Property Constraint** based if the search is based on account properties. For more information, see Adding an Account Discovery rule on page 387. • **Filter Search Location**: If a directory is searched, this is the container within the directory that was searched. • **Auto Manage**: A check mark displays if discovered accounts are automatically added to SPP. • **Set default password**: A check mark displays if the rule causes default passwords to be set automatically. • **Set default SSH key**: A check mark displays if the rule causes default SSH keys to be set automatically.

Property	Description
	• **Assign to Password Profile**: The password profile assigned. • **Assign to Sync Group**: The name of the assigned password sync group. • **Assign to SSH Key Profile**: The name of the assigned SSH Key profile. • **Assign to SSH Key Sync Group**: The name of the assigned SSH Key Sync group. • **Enable Password Request**: A check mark displays if the passwords is available for release. • **Enable Session Request**: A check mark displays if session access is enabled. • **Enable SSH Key Request**: A check mark displays if SSH key request is enabled.

Schedule	Click **Schedule** to control the job schedule.
	Select **Run Every** to run the job along per the run details you enter. (If you clear **Run Every**, the schedule details are lost.)
	• Select a time frame:
	  • **Never**: The job will not run according to a set schedule. You can still manually run the job.
	  • **Minutes**: The job runs per the frequency of minutes you specify. For example, `Run Every 30/Minutes` runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
	  • **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select `Run Every 2/Hours/@ minutes after the hour 15`.
	  • **Days**: The job runs on the frequency of days and the time you enter.
	  For example, `Run Every 2/Days/Starting @ 11:59:00 PM` runs the job every other evening just before midnight.
	  • **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.
	  For example, `Run Every 2/Weeks/Starting @ 5:00:00 AM` and **Repeat on these days** with **MON**, **WED**, **FRI**

Property	Description
	selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday. • **Months**: The job runs on the frequency of months at the time and on the day you specify. For example, If you select `Run Every 2/Months/Starting @ 1:00:00 AM` along with `Day of Week of Month/First/Saturday`, the job will run at 1 a.m. on the first Saturday of every other month. • Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click + **Add** or − **Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap. For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values: Enter `Run Every 10/Minutes` and set **Use Time Windows**: • **Start 10:00:00 PM** and **End 11:59:00 PM** • **Start 12:00:00 AM** and **End 2:00:00 AM** An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time. If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter. For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values: For days, enter `Run Every 2/Days` and set **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**. If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

Downloading a public SSH key

When you add an asset and select the **Automatically Generate the SSH Key** (**SSH Key Generation and Deployment** setting on the **Connection** page in the **Asset** dialog), SPP allows you to download the SSH key so that you can manually install it on the asset.

To download a public SSH key

1. Navigate to **Asset Management** > **Assets**.
2. In **Assets**, select an asset that has an SSH key authentication type.
3. Expand the **SSH Host Key** drop-down, and select **Download SSH Key**. The SSH key will be downloaded according to your browser's file download settings.

Partitions

A partition is a named container for assets that can be used to segregate assets for delegated management. It is the responsibility of the Asset Administrator to add partitions to SPP. Partitions allow you to set up multiple asset managers, each with the ability to define password guidelines for the managed systems in their own workspace. Typically, you partition assets by geographical location, owner, function, or by operating system. For example, SPP can enable you to group Unix assets in a partition and delegate the Unix administrator to manage it. Every partition should have a partition owner. For more information, see Adding a partition on page 358.

You must assign all assets, and the accounts associated with them, to a partition. By default, SPP assigns all assets and their associated accounts to the default partition, but you can set a different partition as the default.

To access **Partitions**:

- web client: Navigate to **Asset Management** > **Partitions**. Select a partition, then click to display additional information and options.

Selecting one of the accounts displays the following information:

- Properties tab (partitions): Displays general information about the selected partition.
- Assets tab (partitions): Displays the assets assigned to the selected partition.
- Accounts tab (partitions): Displays the accounts assigned to the selected partition.
- Owners tab (partitions): Displays information about the owners of the partition.
- Password Profiles tab (partitions): Displays the profiles associated with this partition. When a partition is added, a default asset profile is created for the partition, which can be edited, but not deleted.
- SSH Key Profiles tab (partitions): Displays the SSH key profiles associated with this partition.
- History tab (partitions): Displays the details of each operation that has affected the selected partition.

Use these toolbar buttons to manage partitions.

- **New Partition**: Add a partition to SPP. For more information, see Adding a partition on page 358.
- **Delete**: Remove the selected partition. For more information, see Deleting a partition on page 364.
- **View Details**: Select a partition then click this button to open additional information and options for the partition.
- **Set as Default**: Set a partition as the default. All new assets you add are automatically assigned to the default partition. For more information, see Setting a default partition on page 362.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of partitions.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

About profiles

The profile includes the schedules and rules governing the partition’s assigned assets and the assets' accounts. For example, the profile defines how often a password check is required on an asset or account.

A partition can have multiple profiles, each assigned to different assets, if desired. An account is governed by only one profile. If an account is not explicitly assigned to a profile, the account is governed by the one assigned to the parent asset. If that asset does not have an assigned profile, the partition's default profile is assigned. When updating or restarting a service on a password change, the profile assigned to the asset is used for dependent account service modifications.

When you create a new partition, SPP creates a corresponding default profile with default schedules and rules. You can create multiple profiles to govern the accounts assigned to a partition. Both assets and accounts are assigned to the scope of a profile.

For example, suppose you have an asset with 12 accounts and you configure the profile to check and change passwords every 60 days. If you want the password managed for one of those accounts every seven days, you can create another profile and add the individual account to the new profile. Now, SPP will check and change all the passwords on this asset every 60 days except for this account, which will change every seven days.

Implicit and explicit association

It is important to understand the difference between implicit and explicit assignments to a profile.

Implicit associations

SPP makes implicit assignments. For example, when you add an asset to SPP, it automatically adds the asset to the default partition and assigns it to the scope of the default profile. This is called implicit association. Assets implicitly inherit the partition's default profile. Similarly, accounts inherit their parent asset’s profile. That means when you add an account to an asset, SPP implicitly adds that account to its asset’s profile.

Later, if you reassign the asset to another profile, SPP automatically reassigns all of the asset’s associated accounts to the new profile.

Explicit associations

SPP allows you to explicitly add an asset or an account to a specific profile. When you explicitly assign an asset to a profile, it overrides the implicit inheritance from the partition so the asset's profile is no longer determined by its partition. Similarly, when you explicitly assign an account to a profile, SPP overrides the implicit inheritance from the asset and the account’s profile is no longer determined by its asset.

Now, if you reassign the asset to another profile, SPP will not reassign the asset’s associated accounts that were explicitly assigned to the old profile.

Resetting the default profile

If you set another profile as the default, SPP implicitly reassigns all assets and their associated accounts to that new default, but it will not reassign any assets or accounts that you have explicitly assigned to a profile. Once the implicit inheritance is broken, changing a partition's default profile has no effect on the scope of a profile. For more information, see Setting a default profile.

Related Topics

Assigning assets or accounts to a password profile and SSH key profile

Assigning a profile to an asset

Password Profiles

SSH Key Profiles

How do I manage accounts on unsupported platforms

Properties tab (partitions)

The **Properties** tab lists information about the selected partition.

To access the **Properties** tab, in the web client, navigate to **Asset Management** > **Partitions** > **View Details** > **Properties**.

Table 118: Partitions Properties tab: General properties

Property	Description
Name	The partition name.
Description	Information about the selected partition.

Delete: Click this button to delete the selected partition.

Assets tab (partitions)

The **Assets** tab displays the assets assigned to the selected partition.

Click **+ Add Asset** from the details toolbar to add one or more assets to the selected partition.

To access **Assets**:

- web client: Navigate to **Asset Management** > **Partitions** > (View Details) > **Assets**.

Table 119: Partitions: Assets tab properties

Property	Description
Name	The asset name.
Password Profile	The name of the profile that manages the asset.
SSH Key Profile	The name of the SSH key profile.
Account Discovery Job	The Account Discovery job assigned to discover accounts on this asset that meet the rules criteria. Each asset in a partition can have a separate and unique Account Discovery job.
Asset Discovery Job	The Asset Discovery job assigned to discover assets by searching directory assets, such as Active Directory, or by scanning network IP ranges in the partition that meet the rules criteria. An asset can be read-access available for Asset Discovery jobs beyond partition boundaries. For more information, see Management tab (add asset).
Platform	The platform of the selected asset.
Session Request	A check in this column indicates that session access requests are enabled for the asset.

Property	Description
Disabled	A check in this column indicates the asset is disabled.
Product License	If applicable (for example, for a Windows asset), indicates your license model, such as System or Desktop.
Connection Type	The connection authentication type for the asset, such as Password, SSH Key, Directory Account, Local System Account, and so on. For more information, see Custom Properties.
Description	Descriptive information entered when the asset was added.

Use these buttons on the details toolbar to manage the assets assigned to the selected partition.

Table 120: Partitions: Assets tab toolbar

Option	Description
Add Asset	Add one or more assets to the selected partition.
Delete	Remove the selected asset from the partition.
View Details	Edit the selected asset. Assets that are part of a Directory have the following properties automatically synchronized from the Directory: Name, Description, NetworkAddress.
Access Request	Select **Enable Session Request** to allow session requests for the selected asset. Select **Disable Session Request** to disallow session requests for the selected asset.
SSH Host Key	This option allows you to manually add the host key to an asset in cases where SPP cannot discover the asset automatically (such as for an **Other Directory** asset).
Test Connection	Select to verify that SPP can log in to the asset using the current service account credentials. For more information, see Checking an asset's connectivity on page 336.
Synchronize Now	Run the directory addition (incremental) synchronization process by asset and account. The sync is queued by asset by provider and runs one directory sync on that asset at a time. You can run multiple syncs in parallel on different assets. This is the faster type of directory sync because deletions are not synced. A **Tasks** window displays the progress and outcome of the task. You can click **Details** to see more information or click **Stop** to cancel the task. In addition, this process runs through the discovery, if there are discovery rules and configurations set up.The API (`Assets/Synchronize`) can be used to run the deletion (full) sync which includes all deletions, additions, and changes.

Option	Description
	This sync takes longer (perhaps hours), especially the first time it is run based on your directory setup.
Discover Accounts	Run the Account Discovery job.
Enable-Disable	Select one of the following: Select **Enable** to have Safeguard for Privileged Passwords manage a disabled partition. Select **Disable** to prevent Safeguard for Privileged Passwords from managing the selected partition.
Show Disabled	Display the assets that are not managed and are disabled and have no associated accounts. Asset management can be controlled by selecting an asset and clicking **Enable-Disable**.
Hide Disabled	Hide the assets that are not managed and are disabled and have no associated accounts. Asset management can be controlled by selecting an asset and clicking **Enable-Disable**.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Retrieve and display an updated list of assets associated with the selected partition.
Search	To locate a specific asset in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Related Topics

Adding assets to a partition

Removing assets from a partition

Accounts tab (partitions)

The **Accounts** tab displays the accounts assigned to the selected partition.

> NOTE: By default, all accounts associated with an asset are assigned to the same profile, but you can reassign them. For more information, see Creating a password profile on page 361.

To access **Accounts**:

- web client: Navigate to **Asset Management** > **Partitions** > (View Details) > **Accounts**.

Table 121: Partitions: Accounts tab properties

Property	Description
Name	The account name.
Domain Name	The domain name of the account if the account is an Active Directory account. Used to help determine uniqueness.
Parent	The partition in which the asset where the account resides.
Password Profile	The name of the profile that manages the account.
SSH Key Profile	The name of the SSH key profile that governs the accounts assigned to a partition.
Service Account	A check in this column indicates that the account is a service account.
Password Request	A check in this column indicates that password release requests are enabled for the account.
Session Request	A check in this column indicates that session access requests are enabled for the account.
SSH Key Request	A check in this column indicates that SSH key release requests are enabled for the account.
Disabled	A check in this column indicates the account is disabled.
Password	A ✓ check in this column indicates a password is set for the account. For more information, see Checking, changing, or setting an account password on page 291.
TOTP Authenticator	A ✓ check in this column indicates a TOTP Authenticator is set for the account. For more information, see Setting a TOTP authenticator.
SSH Key	A ✓ check in this column indicates an SSH key is set for the account. For more information, see Checking, changing, or setting an SSH key on page 292.
API Keys	A ✓ check in this column indicates an API key is set for the account. For more information, see Checking, changing, or setting an SSH key on page 292.
Description	Descriptive information entered when the account was added.
Tags	The tags associated with the account.

Use these buttons on the details toolbar to manage the accounts assigned to the selected partition.

Table 122: Partitions: Accounts tab toolbar

Option	Description
New Account	Add accounts to the selected partition. For more information, see Adding an account to a partition.
Delete	Remove the selected account from the partition.
View Details	View additional information on the selected account.
Account Secrets	Menu options include: • **Check Password** • **Change Password** • **Check SSH Key** • **Change SSH Key**
Access Request	Select an option to enable or disable access request services for the selected partition. Values are derived from whether the platform of the asset indicates it supports any of the following: Password Request, SSH Key Request, Session Request. You can enable or disable Password Request, Session Request, and SSH Key Request, as needed. Service Accounts are created when the Asset is created and by default are not enabled for session or password access. Discovered Accounts are controlled by the Account Discovery template that is used in discovering the accounts. They are a property of the rule template of the Account Discovery job. For more information, see Adding an Account Discovery rule on page 387.
Discover SSH Keys	Run the SSH Key Discovery job associated with the account.
Enable-Disable	Select **Enable** to have Safeguard for Privileged Passwords manage a disabled partition. Select **Disable** to prevent Safeguard for Privileged Passwords from managing the selected partition.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of asset accounts.
Search	To locate a specific asset account or set of accounts in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Owners tab (partitions)

The **Owners** tab displays information about the directly managed objects associated with the partition.

To access **Owners**:

- web client: Navigate to **Asset Management** > **Partitions** > (View Details) > **Owners**.

Table 123: Partitions: Owners tab properties

Property	Description
Type	The type of object.
Name	The name of the user or user groups.
Provider	The name of the authentication provider.

Use the following buttons on the details toolbar to manage the objects owned by the selected partition.

Table 124: Partitions: Owners toolbar

Option	Description
Add User/User Groups	Add one or more users or user groups to the selected partition. For more information, see Adding users or user groups to a partition.
Remove Selected	Remove the selected object from being managed by the selected partition.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of managed objects.
Search	To locate a specific object in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Asset Administrators and Auditors can also generate reports showing more detailed information on the ownership of specific objects (including effective ownership). For more information, see Ownership reports.

Password Profiles tab (partitions)

The **Password Profiles** tab lists the password profiles associated with this partition. for more information, see About profiles. You can create a password profile then add assets and accounts to the password profile. For more information, see Assigning assets or accounts to a password profile and SSH key profile.

Click **+ New Profile** from the details toolbar to add a password profile to the selected partition. For more information, see Creating a password profile on page 361.

To access **Password Profile**:

- web client: Navigate to **Asset Management** > **Partitions** > (View Details) > **Password Profile**.

Table 125: Partitions: Password Profiles tab properties

Property	Description
Default	"Default" displays in this column for the default password profile. For more information, see Setting a default profile on page 363.
Name	Password management password profile name.
Check Password	The check password setting used to verify account passwords. For more information, see Check Password on page 414.
Change Password	The change password setting used to to verify account passwords. For more information, see Change Password on page 417.
Password Rule	The account password rule that governs the construction of the new password created by Safeguard for Privileged Passwords during automatic password change. For more information, see Account Password Rules on page 424.
Description	Information about the selected password profile.

Use these buttons on the details toolbar to manage the partition's password profiles.

Table 126: Partitions: Password Profiles tab toolbar

Option	Description
+ New Profile	Add a password profile to the selected partition. For more information, see Creating a password profile on page 361.
Delete	Remove the selected password profile. If you delete a password profile, Safeguard for Privileged Passwords reassigns all assets and accounts to the default password profile.

Option	Description
View Details	View additional details for the selected password profile.
Set as Default	Set the selected password profile as the default password profile. For more information, see Setting a default profile on page 363.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of password profiles.
Search	To locate a specific password profile or set of password profiles in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

SSH Key Profiles tab (partitions)

Each managed account can have a single SSH identity key. An SSH key can be requested and configured for A2A (account level scoping) and used for sessions.

The **SSH Key Profiles** tab lists the SSH key profiles associated with the selected partition. For more information, see About profiles on page 346.

To access **SSH Key Profiles**:

- web client: Navigate to **Asset Management** > **Partitions** > (View Details) > **SSH Key Profiles**.

Table 127: Partitions: SSH Key Profiles tab properties

Property	Description
Default	**Default** displays in this column to identify the default profile. For more information, see Setting a default profile on page 363.
Name	SSH key profile name.
Check SSH Key	The **Check SSH Key** setting used to verify SSH keys. For more information, see Check SSH Key settings on page 435.
Change SSH Key	The **Change SSH Key** setting used to verify SSH keys. For more information, see Change SSH Key settings on page 438.
Discover SSH Key	The SSH Key Discovery job used to discover the SSH keys. For more information, see Discover SSH Key settings on page 444.
Description	Information about the selected SSH key profile.

Use these buttons on the details toolbar to manage your partitions profiles.

Table 128: Partitions: SSH Key Profiles tab toolbar

Option	Description
New Profile	Add an SSH key profile to the selected partition. For more information, see Creating an SSH key profile on page 362.
Delete	Remove the selected SSH key profile. If you delete an SSH key profile, SPP reassigns all assets and accounts to the default profile. If no default profile is set, SPP will remove the assets and accounts along with the profile.
View Details	Modify the selected SSH key profile.
Set as Default	(Optional) Set the selected profile as the default profile. Once a default profile has been selected, there will always be a default profile (which profile is the default can be changed at any time, but a default profile will always be needed for the partition). The only way to stop requiring a default profile be selected is to remove all SSH profiles from the partition. For more information, see Setting a default profile on page 363.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of SSH key profiles.
Search	Locate a specific SSH key profile or set of profiles in this list by entering the character string to be used to search for a match. For more information, see Search box on page 78.

History tab (partitions)

The **History** tab allows you to view or export the details of each operation that has affected the selected partition.

To access **History**:

- web client: Navigate to **Asset Management** > **Partitions** > (View Details) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.

- **Refresh**: Update the list displayed.
- **Search**: For more information, see Search box on page 78.

Table 129: Partitions: History tab properties

Property	Description
Date/Time	The date and time of the event.
User	The display name of the user that triggered the event.
Source IP	The network DNS name or IP address of the managed system that triggered the event.
Object Name	The name of the selected partition.
Event	The type of operation made to the selected partition: • Create • Delete • Update • Add Membership • Remove Membership NOTE: A membership operation indicates a "relationship" change with a related or parent object such as a delegated administrator was added or removed from the selected partition.
Related Object	The name of the related object.
Related Object Type	The type of the related object.
Parent	The name of the object to which the selected partition is a child.
Parent Object Type	The parent object type.

Managing partitions

Use the controls and tabbed pages on the Partitions page to perform the following tasks to manage partitions:

- Adding a partition
- Adding assets to a partition
- Removing assets from a partition
- Adding users or user groups to a partition
- Creating a password profile
- Creating an SSH key profile

- Setting a default profile
- Assigning assets or accounts to a password profile and SSH key profile
- Deleting a partition
- Setting a default partition

Adding a partition

It is the responsibility of the Asset Administrator to add partitions to SPP. When you create a new partition, SPP creates a corresponding default profile with default schedules and rules. For more information, see Setting a default profile on page 363.

To add a partition

1. Navigate to **Asset Management** > **Partitions**.
2. Click **+ New Partition** from the toolbar.
3. In the **Partition** dialog, enter the following information:
   a. **Name**: Enter a unique name for the partition. Limit: 50 characters.
   b. **Description**: (Optional) Enter information about this partition. Limit: 255 characters.
4. Click **OK** to save the partition.

When you create a new partition, SPP creates a corresponding default profile with default schedules and rules. You can:

- Modify the profile for the partition you created.
- Change the default profile. For more information, see Setting a default profile on page 363.

Adding assets to a partition

Use the **Assets** tab on the **Partitions** view to add one or more assets to a partition. When you assign an asset to a partition, all the accounts associated with that asset are assigned to that partition, as well.

You can only assign an asset to one partition at a time. When you assign an asset to a partition, all accounts associated with that asset are automatically reassigned to that partition, as well. Then, any new accounts you add for that asset are automatically assigned to that partition.

You can reassign the asset to another partition either from the scope of the other partition or from an asset's **General** properties. For more information, see Assigning an asset to a partition on page 336.

When you associate an asset to a partition, all the accounts associated with that asset, are also added to the scope of that partition. For more information, see About profiles on page 346.

To add assets to a partition

1. Navigate to **Asset Management** > **Partitions**.
2. In **Partitions**, select a partition from the object list and click **Edit**.
3. Open the **Assets** tab.
4. Click **+ Add Asset** from the details toolbar.
5. On the **Select assets to add to partition** dialog, select one or more assets.
6. Click **Select Assets**.

If you do not see the asset you are looking for and are an Asset Administrator, you can create it in the dialog by clicking **+ New Asset**. For more information, see Adding an asset.

Adding an account to a partition

On the web client, use the **Accounts** tab on the **Partitions** view to add an account to a partition.

You can manage tasks and services on a domain controller (DC) asset. For more information, see Using a domain controller (DC) asset on page 299.

To add an account to an asset

1. Navigate to **Asset Management** > **Partitions**.
2. Select a partition and click **View Details**.
3. Open the **Accounts** tab.
4. Click **+ New Account** from the details toolbar.
5. In the **Select the asset for the new account** dialog, select an asset to associate with this account then click **Select Asset**.
6. In the **New Account** dialog, enter the following information:
    - On the **General** tab:
        - **Name**:
            - Local account: Enter the login user name for this account. Limit: 100 characters.
            - Directory Account: **Browse** to find the account.
        - **Description**: (Optional) Enter information about this managed account. Limit: 255 characters.
    - On the **Management** tab:
        - **Enable Password Request**: This check box is selected by default, indicating that password release requests are enabled for this account. Clear this option to prevent someone from requesting the password for

this account. By default, a user can request the password for any account in the scope of the entitlements in which they are an authorized user.

- **Enable Session Request**: This check box is selected by default, indicating that session access requests are enabled for this account. Clear this option to prevent someone from requesting session access using this account. By default, a user can make an access request for any account in the scope of the entitlements in which they are an authorized user.
- **Available for use across all partitions** (Only available for some types of directory accounts): When selected, any partition can use this account and the password is given to other administrators. For example, this account can be used as a dependent account or a service account for other assets. Potentially, you may have assets that are running services as the account, and you can update those assets when the service account changes. If not selected, partition owners and other partitions will not know the account exists. Although archive servers are not bound by partitions, this option must be selected for the directory account for the archive server to be configured with the directory account.

7. Click **OK**.

Removing assets from a partition

You cannot remove assets from a partition.

You can reassign the asset to another partition either from the scope of the other partition or from an asset's **General** properties. For more information, see Assigning an asset to a partition on page 336.

When you associate an asset to a partition, all the accounts associated with that asset, are also added to the scope of that partition. For more information, see About profiles on page 346.

Adding users or user groups to a partition

When you add users to a partition, you are specifying the users or user groups that have ownership of a partition.

It is the responsibility of the Asset Administrator to add users and user groups to partitions. The Security Policy Administrator only has permission to add groups, not users. For more information, see Administrator permissions on page 604.

To add users to a partition

1. Navigate to **Asset Management** > **Partitions**.
2. In **Partitions**, select a partition from the object list and click **View Details**.
3. Open the **Owners** tab.

4. Click + **Add**.
5. Select one or more users or user groups from the list in the **Users/User Groups** dialog.
6. Click **Select Owners** to save your selection.

Creating a password profile

It is the responsibility of the Asset Administrator or the partition's delegated administrator to add password profiles to partitions.

To add a password profile to a partition

1. Navigate to **Asset Management** > **Partitions**.
2. In **Partitions**, select a partition from the object list and click **View Details**.
3. Open the **Password Profiles** tab.
4. Click +**New Profile** from the details toolbar.
5. On the **General** tab, supply the following information:
   a. **Name**: Enter a unique name for the profile. Limit: 50 characters
   b. **Description**: Enter information about this profile. Limit: 255 characters
6. On the **Check Password** tab, select a previously defined check password setting from the drop-down menu or click + **Add** to add a new check password setting. These are the rules used to verify account passwords. For more information, see Adding check password settings on page 415.
7. On the **Change Password** tab, select a previously defined change password setting from the drop-down menu or click + **Add** to add a new change password setting. These are the rules used to reset account passwords. For more information, see Adding change password settings on page 418.
8. On the **Account Password Rule** tab, select a previously defined account password rule or click + **Add** to add a new account password rule. An account password rule is a complexity rule that governs the construction of the new password created by SPP during an automatic password change. For more information, see Adding an account password rule on page 425.
9. Click **OK** to save your selections and create the profile.
10. When creating a new profile, the **Password Sync Groups** tab is not available. This tab is displayed while editing a profile. You can use the **Password Sync Groups** tab to add or update a password sync group governed by the profile change schedule. For more information, see Password sync groups on page 427.

Creating an SSH key profile

It is the responsibility of the Asset Administrator or the partition's delegated administrator to add SSH key profiles to partitions.

To add an SSH key profile to a partition

1. Navigate to **Asset Management** > **Partitions**.
2. In **Partitions**, select a partition from the object list and click **View Details**.
3. Open the **SSH Key Profiles** tab.
4. Click **+New Profile** from the details toolbar.
5. On the **General** tab, supply the following information:
   a. **Name**: Enter a unique name for the profile. Limit: 50 characters
   b. **Description**: Enter information about this profile. Limit: 255 characters
6. On the **Check SSH Key** tab, select a previously defined check SSH key setting from the drop-down menu. These are the rules SPP uses to verify account SSH keys. For more information, see Adding SSH key check settings on page 436.
7. On the **Change SSH Key** tab, select a previously defined change SSH key setting from the drop-down menu. These are the rules used to reset account SSH keys. For more information, see Adding SSH key change settings on page 439.
8. On the **Discover SSH Key** tab, select a previously defined discover SSH key settings selection. These are the rules used to discover SSH keys. For more information, see Adding SSH key discovery on page 445.
9. Click **OK** to save your selections and create the profile.

When creating a new partition SSH key profile, the **SSH Key Sync Groups** tab is not displayed. This tab is displayed while editing a partition SSH key profile. You can use the **SSH Key Sync Groups** tab to add or update an SSH key sync group governed by the profile change schedule. For more information, see SSH Key Sync Groups settings on page 446.

Setting a default partition

Each Asset Administrator can set a unique default partition and profile so that all new assets that administrator adds are automatically assigned to the default partition and default profile. For more information, see Setting a default profile on page 363.

To set the default partition

1. Navigate to **Asset Management** > **Partitions**.
2. In **Partitions**, select a partition and click **Set as Default** from the toolbar.

Setting a default profile

When you create a new partition, SPP creates a corresponding default profile with default schedules and rules. Each Asset Administrator can set a unique default partition and profile. Once you set a default profile, all new assets and accounts you add are automatically assigned to that profile.

SPP sets the default schedules to "Never" verify or reset passwords or SSH keys.

When you associate an asset to a partition, all the accounts associated with that asset, are also added to the scope of that partition. For more information, see About profiles on page 346.

To set another profile as the default

1. Navigate to **Asset Management** > **Partitions**.
2. In **Partitions**, select a partition and click **View Details**.
3. Open the **Password Profiles** or **SSH Key Profiles** tab.
4. Select a profile that is not the current default and click **Set as Default** from the details toolbar or context menu. (When you select the default profile, the **Set as Default** icon is grayed out.)

Assigning assets or accounts to a password profile and SSH key profile

You can assign an asset or an account to a password profile, an SSH key profile, or both. The assets and accounts must be in the scope of the partition to be assigned to a profile.

You can also configure SPP to run automatic Asset Discovery or Account Discovery jobs. For more information, see Discovery on page 364.

CAUTION: Only associate accounts to a profile that you want Safeguard for Privileged Passwords to manage.

To add assets or accounts to a profile

1. Navigate to **Asset Management** > **Partitions**.
2. Select a partition from the object list and click **View Details**.
3. Open the **Password Profiles** or **SSH Key Profiles** tab.
4. Select a profile and click **Edit**.
5. To add an asset to the selected profile, switch to the **Assets** tab.
6. Select the asset(s) to be added.
7. To add an account to the selected profile, switch to the **Accounts** tab.
8. Select the account(s) to be added.

9. Once you have finished editing the profile, save and exit by clicking outside of the profile dialog.

Deleting a partition

When deleting a partition, you must designate another partition to transfers all assets and accounts. The profiles and associated profile settings, discovery jobs, and history data for the partition you are deleting are deleted along with the profile.

To delete a partition

1. Navigate to **Asset Management** > **Partitions**.
2. Select the partition to be deleted.
3. Click 🗑 **Delete**.
4. In the dialog, select the partition where assets and accounts are to be reassigned.
5. Click **Select Partition** to reassign the assets and accounts and delete the selected partition.

Discovery

Safeguard for Privileged Passwords discovery jobs can find assets, accounts, SSH keys, and services in your network environment. This can simplify initial deployment and ongoing maintenance of the privileged accounts in your network environment.

Details on the jobs follow.

- **Asset Discovery**: Asset Discovery jobs find assets by searching directory assets, such as Active Directory, or by scanning network IP ranges. Rules control which assets are found. Asset Discovery jobs can be scheduled to run on regular intervals. The discovery job can be configured with templates to set default settings on newly created assets including connection details. The assets created by discovery jobs are considered to be managed by Safeguard, but this has no effect on the network asset. An asset with valid connection information can be used for account discovery.

  If you use **Directory** as the asset discovery **Method**, directory assets that are shared can be discovered into any partition. To share a directory asset, select **Available for discovery across all partitions** for the asset; see Management tab (add asset).

- **Account Discovery**: Account Discovery jobs find accounts by searching directory assets such as Active Directory or by scanning local account databases on Windows and Unix assets (`/etc/passwd`) that are associated with the account discovery job. Rules control which accounts are found. Account discovery jobs can be scheduled to run on regular intervals. The discovery job can be configured to set default settings on newly created accounts. Accounts found by account discovery are neither

managed nor disabled until you decide to manage them or disable them. If an account is managed by Safeguard, this means the password can be managed according to the profile settings associated with the discovery job. Safeguard can make the account available for password and/or session requests according to configured entitlements and policy.

The accounts in the scope of the discovery job may include accounts that were previously added (manually) to the Safeguard partition. For more information, see Adding an account on page 286.

- **Service Discovery**: Service Discovery jobs find Windows services that run as accounts managed by Safeguard. If Safeguard is managing the service account password, Safeguard can update the Windows service configuration to match the password when the password changes and restart the service automatically.
- **SSH Key Discovery**: SSH Key Discovery jobs search user directories and discover the authorized SSH keys in managed accounts.

In the web client, information on all discovered items is shown by default. You can also use the **Partition** drop-down to select a specific partition to view information on.

The following tiles are displayed in the **Discovered Items** section:

- **Accounts**: This displays the number of discovered accounts. Click the tile for detail.
- **Services**: This displays the number of discovered services. Click the tile for detail. You can launch discover service account jobs from **Asset Management** > **Assets** > (View Details) > **Discovered Services**. For more information, see Discovered Services tab (asset) on page 312.
- **SSH Keys**: This displays the number of discovered SSH keys. Click the tile for detail.

The **Discovery Jobs** section is broken into the follow tabs:

- **Assets** tab: This tab shows the Asset Discovery jobs available to run against the directories or networks to discover assets for potential management displays.
- **Accounts** tab: This tab shows the Account Discovery jobs available to run against the in scope assets to discover accounts for potential management displays.
- **SSH Keys** tab: This tab shows the SSH Key Discovery jobs available to run against the managed accounts to discover SSH keys for potential management displays.

Asset Discovery

You can schedule one or more Asset Discovery jobs to run automatically against the directories or network (IP range) you have added to SPP. The assets in the scope of the discovery job may include assets that were previously added (manually) to the Safeguard partition. For more information, see Adding an asset.

If you use **Directory** as the asset discovery **Method**, directory assets that are shared can be discovered into any partition. To share a directory asset, select **Available for discovery across all partitions** for the asset; see Management tab (add asset).

When an Asset Discovery job runs, the found asset is added to Assets. If the operating system cannot be detected in the Asset, Network Scan or Directory method of asset discovery, the **Linux** operating system is applied which you can modify later.

For more information, see Asset Discovery job workflow on page 367.

Properties and toolbar

Go to Asset Discovery:

- web client: Navigate to **Asset Management** > **Discovery** > **Assets**

Use these toolbar buttons to manage the discovery job settings.

Table 130: Asset Discovery: Toolbar

Option	Description
New Asset Discovery Job	Add an Asset Discovery job. For more information, see Adding an Asset Discovery job on page 368.
Delete	Delete the selected Asset Discovery job.
View Details	Modify the selected Asset Discovery job. You can also double-click a row to open the edit dialog.
Run Now	Run the selected Asset Discovery job. A **Task** pop-up display which shows the progress and completion.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of Asset Discovery jobs that have run.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 78.

Asset Discovery jobs display in the grid.

Table 131: Asset Discovery: Asset Discovery job grid

Name	Name of the discovery job
Created by	The creator of the job.
Discovery Type	The type of job, for example, Windows, Unix, or Directory
Directory	The directory on which the discovery job runs
Partition	The partition in which to manage the discovered assets or assets
Schedule	Designates when the Asset Discovery job runs

Last Run Date	The date the selected Asset Discovery job ran
Next Run Date	The date when the Asset Discovery job is scheduled to run next
Last Success Run Date	The most recent date the selected Asset Discovery job successfully ran
Last Failure Run Date	The most recent date the selected Asset Discovery job failed

Asset Discovery job workflow

You can configure, schedule, test, and run Asset Discovery jobs. After the job has run, you can select whether to manage the asset. You can also view information about the Asset Discovery jobs that have run.

Asset Discovery job workflow

1. Create an Asset Discovery job. For more information, see Adding an Asset Discovery job on page 368.
2. After you save the Asset Discovery job, you can test it by selecting **Run Now**. For more information, see Asset Discovery on page 365.
3. After the Asset Discovery job runs, select the asset discovery job and click **View Details**. For more information, see Asset Discovery Results on page 381.
4. To control management of an asset, navigate to **Asset Management** > **Assets**, select the asset, and choose one of these context menu options.

Enable	Select **Enable** to have SPP manage a disabled asset. This option is only available for assets that have been disabled.
Disable	Select **Disable** to prevent SPP from managing the selected asset. When you disable an asset, SPP disables it and removes all associated accounts. If you choose to manage the asset later, SPP re-enables all the associated accounts.

5. On **Asset Management** > **Assets**, you can show or hide assets marked as disabled, use the following buttons. For more information, see Assets on page 298.

Show Disabled	Display the disabled assets.
Hide Disabled	Hide assets marked as disabled.

6. Search the Activity Center for information about discovery jobs that have run. SPP lists the Asset Discovery events in the **Asset Discovery Activity** category.

Adding an Asset Discovery job

You can add a new Asset Discovery job.

To add an asset discovery job

1. Navigate to **Asset Management** > **Discovery**.
2. Open the **Assets** tab.
3. Click **+New Asset Discovery Job** to create a new Asset Discovery job.
4. In the **New Asset Discovery Job** dialog, provide information for the discovery job on the following tabs:

General tab (asset discovery)	Where you add general information about the discovery job and identify which partition you want SPP to add the assets it discovers.
Information tab (asset discovery)	Where you select the directory and set the search location.
Asset Discovery Rules tab (asset discovery)	Where you define the search constraints and conditions, add tags, and choose the profile you want to govern the discovered assets.
Schedule tab (asset discovery)	Where you configure the schedule for the discovery job.

After you save the discovery job, you can modify or run it using the **Asset Discovery** toolbar. For more information, see Asset Discovery.

General tab (asset discovery)

Navigate to:

- web client: **Asset Management** > **Discovery** > **Assets** > (add or edit a Asset Discovery job).

On the **General** tab, supply general information about the Asset Discovery job and identify the partition where you want SPP to add the assets it discovers.

Table 132: Discovery: General properties

Property	Description
Name	Enter a name for the Asset Discovery job. Limit: 50 characters
Description	Enter information about this Asset Discovery job.

Property	Description
	Limit: 255 characters
Partition	Use **Browse** to select the partition in which to manage the discovered assets. You can also add a new partition from the **Partitions** dialog (accessed via the **Browse** button) by clicking + **Create New**. IMPORTANT: You cannot change the partition after you save this discovery job.

Information tab (asset discovery)

Navigate to:

- web client: **Asset Management** > **Discovery** > **Assets** > (add or edit a Asset Discovery job).

On the **Information** tab, define the directory or network information for the discovery job.

Table 133: Discovery Type

Property	Description
Discovery Type	Choose a type of discovery: • **Asset** • **Directory** • **Network** • **StarlingAgent** If you select **Directory**, directory assets that are shared can be discovered into any partition. Directories include Active Directory or LDAP. See *Directories that can be searched* in Supported platforms. To share a directory asset, select **Available for discovery across all partitions** for the asset; see Management tab (add asset). If the check box is not selected, the asset is not shared and the asset will only be discovered into the partitions to which the directory asset is assigned.

Table 134: Discovery: Information properties for Asset scans

Property	Description
ESX Host (RegEx)	Enter a value to limit the search to selected ESX hosts that match this regular expression.

Property	Description
Asset	Select an asset in the current partition to run the Asset Discovery job. An asset is only available for selection if the platform supports Local Asset Discovery.
Ignore If Not Running	Select this check box to limit the search to virtual machines that are currently running.

Table 135: Discovery: Information properties for Directory scans

Property	Description
Directory	Select the **Directory** on which to run the Asset Discovery job.

Table 136: Discovery: Information properties for Network scans

Property	Description
Enable OS Detection	This check box is selected by default, indicating that OS fingerprinting is to be used to detect the operation system being used. Clear this check box if you do not want to use the OS fingerprinting process.
Starting IP Address	Enter a starting IPv4 address. All IPv4 addresses between this IPv4 address and the IPv4 address entered in the Ending IP Address field will be included in the discovery. NOTE: IPv6 scans are not supported.
Ending IP Address	Enter an ending IPv4 address. All IPv4 addresses between this IPv4 address and the IPv4 address entered in the Starting IP Address field will be included in the discovery. NOTE: IPv6 scans are not supported.
Exclude IP	SPP allows you to exclude an IP address within a specified IPv4 range from the scan. Click **+ Add** to exclude an IP address from the scan. Click **− Delete** to remove the corresponding excluded IPv4 address and include that IP address in the scan.

Asset Discovery Rules tab (asset discovery)

Navigate to:

- web client: **Asset Management** > **Discovery** > **Assets** > (add or edit a Asset Discovery job).

Use the **Asset Discovery Rules** tab to govern the discovered assets.

Discovery details

- Once SPP creates an asset, it will not attempt to re-create it or modify the asset if the asset is rediscovered by a different job.
- Any SSH host keys encountered in discovery will be automatically accepted.
- You can configure multiple rules for an Asset Discovery job. When SPP runs the Asset Discovery job, if it finds an asset with more than one rule, it applies the connection and profile settings of the first rule that discovers the asset.

To add a new Asset Discovery rule

1. On the **Asset Discovery Rules** tab, click ✎ **Edit**.
2. Click + **Add**.
3. In the **New Asset Discovery Rule** dialog, enter a **Name** up to 50 characters.
4. You must specify at least one condition, the connection, and a profile for each rule:
   a. Under **Conditions**, click Add Condition (asset discovery) to add one or more **Group**, **Constraints**, **LDAP Filter** (for LDAP or Active Directory), or **Find All**. For more information, see Add Condition (asset discovery).
   b. A **Connection Template** is required and defaults to **Use Discovered Platform** (no credentials are associated). To change this, deselect the check box.
   c. On the **Management** tab, you can manage the profiles to govern the discovered assets.
      - The password profile:
        - Defaults to the partition default password profile set on the Password Profiles tab (partitions) or the default partition set at the Partitions level.
        - Is based on the partition selected on the General tab (asset discovery).
        - Allows for creating new password profiles (using + **New Profile**).
      - You may select **SSH Key Profile** to select or create an SSH key profile.
      - You may select **Account Discovery Job** to select or create an account discovery job.
      - For **Managed Network**, you can select the managed network assigned for workload balancing.
   d. Use the **Tags** tab to add rule-based tags. To add a tag to the rule, click + **Add Tag** and enter the tag.
5. Click **Apply** to save the Asset Discovery rule.

Add Condition (asset discovery)

An Asset Discovery rule can have more than one condition, and each condition can have one or more constraints. When SPP runs the discovery job, it finds all assets that meet all of

the search conditions.

Navigate to:

- web client: **Asset Management** > **Discovery** > **Assets** > (add or edit Asset Discovery job) > **New Asset Discovery Job** dialog > **Asset Discovery Rules** tab > (add asset discovery rule) > **New Asset Discovery Rule** dialog > **Conditions** tab > (add condition).

To add Find All condition

1. In the **Condition** dialog, in **Find By**, choose **Find All**.
   - If you are setting up an Asset Discovery job for a directory, **Browse** the **Filter Search Location** to select a container within the directory to search for assets. Select **Include objects from sub containers** to include objects from sub containers or clear the check box to exclude child objects from discovery.
   - If you are setting up an Asset Discovery job for an asset, you can limit the search to selected ESX hosts, and/or virtual machines that are currently running.
2. Click **Preview** to test the conditions you have configured and display a list of assets SPP will find in the directory or network you specified based on the conditions entered.
3. Click **OK.**

To add LDAP Filter (for LDAP or Active Directory) condition

Search base limits the search to the defined branch of the specified directory, including sub containers if that option is selected. This condition is only available for a **Directory** discovery job (LDAP or Active Directory directories).

1. In the **Condition** dialog:
   a. **Find By**: Choose **LDAP Filter** and enter the search criteria to be used.
   b. **Filter Search Location**: **Browse** to select a container within the directory to search for assets.

      TIP: Do not select the Directory Root for Asset Discovery jobs.

   c. **Include objects from sub containers**: Optionally, select this check box to search for assets in sub-containers.
2. Click **Preview** to test the conditions you have configured.
3. Click **OK** to save your selections.

To add Group for a Directory condition

This condition is only available for a **Directory** discovery job.

1. In the **Condition** dialog:
   a. **Find By**: Choose **Group**.
   b. Click **+Add** to launch the **Group** dialog.
   c. **Contains**: Enter a full or partial group name and click **Search**. You can only enter a single string (full or partial group name) at a time.
   d. **Filter Search Location**: **Browse** to select a container to search within the directory.
   e. **Include objects from sub containers**: Select this check box to include child objects.
   f. **Select the group to add**: The results of the search displays in this grid. Select one or more groups to add to the discovery job.
2. Click **Preview** to test the conditions you have configured and display a list of assets Safeguard for Privileged Passwords will find in the directory or network you specified based on the conditions entered.
3. Click **OK** to save your selections.

To add Constraints condition

1. In the **Condition** dialog, in **Find By**, choose **Constraints**.
2. To change the **Filter Search Location**, click **Browse** and select the search location that is the scope of the search. Network Scan Asset Discovery jobs don't support the search bases settings.
3. To apply constraints (search criteria):
   a. Select a property:
      - **Name**
      - **Description**
      - **Network Address**
      - **Operating System**
      - **Operating System Version**

      NOTE: For Network Scan, you can only apply constraints on the information the network finds, which is **Name** and **Operating System**.
   b. Select an operator:
      - **Equals**
      - **Does Not Equal**
      - **Starts With**
      - **Ends With**
      - **Contains**
      - **Does Not Contain**

c. In the **Value** field, type a value of up to 255 characters. The search is not case-sensitive and does not allow wild cards.

4. Click **Preview** to test the conditions you have configured and display a list of assets SPP will find in the directory or network you specified based on the conditions entered.
5. You can add or delete search constraints:
   a. Click **+Add** to additional constraints to your search criteria.
   b. Click **−Delete** to remove the corresponding constraint from your search criteria.
6. Click **OK** to save your selections.

Edit Connection Template (asset discovery)

You can change how you want SPP to connect to and communicate with the discovered assets. The default **Connection Template** is **None**, meaning assets are authenticated manually.

Navigate to:

- web client: **Asset Management** > **Discovery** > **Assets** > (add or edit Asset Discovery job) > **New Asset Discovery Job** dialog > **Asset Discovery Rules** tab > (add asset discovery rule) > **New Asset Discovery Rule** dialog > **Connection Template** tab

Discovery details

- Once SPP creates an asset, it will not attempt to re-create it or modify the asset if the asset is rediscovered by a different job.
- Any SSH host keys encountered in discovery will be automatically accepted.
- You can configure multiple rules for an Asset Discovery job. When SPP runs the Asset Discovery job, if it finds an asset with more than one rule, it applies the connection and profile settings of the first rule that discovers the asset.

To edit connection template information

1. Navigate to the **New Asset Discovery Rule** dialog, and open the **Connection Template** tab.
2. In the **Connection Template** tab, **Use Discovered Platform** is selected by default. By deselecting this option, you can select a different platform using the **Platform** field and may need to completed additional information based on the product selected.
3. Select an **Authentication Type** and complete the information required for your selection.
   - **SSH Key**: To authenticate to the asset using an SSH authentication key, select the **SSH Key Generation and Deployment Settings**:

- **Automatically Generate and deploy a new SSH Key**: Select this option to generate and deploy a new SSH authentication key.
- **Automatically Generate a new SSH Key that I will deploy myself**: Select this option to generate the SSH authentication key and manually append this public key to the authorized keys file on the managed system for the service account. For more information, see For more information, see Downloading a public SSH key on page 344..

  NOTE: The SSH authentication key becomes available after SPP creates the asset. If you do not select this option, SPP automatically installs the SSH authentication key. If you do select this option, SPP creates the key and associates it with the SPP asset you are creating, but it does not install it on the managed system for you.

- **Import an SSH Key that I will deploy myself**: Select this option, then **Browse** to import an SSH authentication key and enter the **Password**. The private key will be associated with the service account.

  NOTE: SPP does not currently manage the options for an authorized key. If an imported key has any options configured in the authorized keys file on the asset, these options will not be preserved when the key is rotated by SPP.

- The following display based on whether you are generating or importing the SSH key:
  - **SSH Key**: (Import) Click **Browse** to select the SSH key to import. On the **Import SSH Key** dialog, browse for the **Private Key File** and enter the **Password**.
  - **Key Comment**: Enter a meaningful comment. If left blank, the comment will default to `Generated by Safeguard`.
  - **Service Account Name**: Enter the name of the service account.
  - **Password**: (Automatic generation) Enter the password.
  - **Service Account Password Profile** can be edited or removed. Available profiles are based on the partition selected on the General tab (asset discovery).
  - **Service Account SSH Key Profile** can be edited or removed. Available profiles are based on the partition selected on the General tab (asset discovery).

- **Directory Account**: To authenticate to the assets using the service account from an external identity store such as Microsoft Active Directory, select the service account.
  - **Account Name**: Click **Browse** to choose the directory account.
  - **Service Account Password Profile** can be edited or removed. Available profiles are based on the partition selected on the General tab (asset discovery).

- **Password**: To authenticate to the assets using a local service account and password.
  - **Account Name** and **Password**: Enter these values.
  - **Service Account Password Profile** can be edited or removed. Available profiles are based on the partition selected on the General tab (asset discovery).
- **Starling Connect**: To authenticate to the assets using Starling Connect.
  - **Account Name** and **Password**: Enter these values.
- **None**: The accounts associated with the asset are not managed and no asset related credentials are stored.

4. The following information may be needed, based on the **Authentication Type** selected.
   - **Login with service account name only**: Selecting this option will allow SPP to login the asset using only the service account name. The domain will not be used.
   - **Privilege Elevation Command**:

     If required, enter a privilege elevation command (such as `sudo`). This is used as a prefix for commands that require privileged access on the system and to manage accounts on Unix-based systems; that is, to check and change SSH keys and to discover accounts.

     Sudo commands follow.

     - AuthorizedKeyCommand

       Specify a program to look up the user's public keys
     - cat
     - chmod
     - chown
     - cp
     - echo
     - egrep
     - find
     - grep
     - host
     - ls
     - mkdir
     - mv
     - rm
     - sed

- sshd
- ssh-keygen
- tee
- test
- touch
- usermod

When adding an asset, this command is used to perform **Test Connection**. For more information, see About Test Connection on page 322.

The privilege elevation command must run non-interactively, that is, without prompting for a password. For more information, see Preparing Unix-based systems on page 628.

The limit is 255 characters.

- **Port**: Enter the port number for the connection.
- **Allow Session Requests**: This check box is selected by default indicating that authorized users can request session access for the discovered assets. Clear the check box if you do not want to allow session requests for the asset.
  - **RDP Port**: Specify the access port on the target server to be used for RDP session requests.
  - **SSH Port**: Specify the access port on the target server to be used for SSH session requests.
- **Connection Timeout**: Enter how long to wait (in seconds) for both the connect and command timeout.
- **Privilege Level Password**: Enter the system enable password to allow access to the configuration.
- **Client ID**: Enter the application Client ID (for example, for ServiceNow or SAP).
- **Use SSL Encryption**: Select this option to enable Safeguard to encrypt communication with this asset. If you do not select this option for a MicrosoftSQL Server that is configured to force encryption, **Test Connection** will use untrusted encryption and succeed with valid credentials. For more information about how Safeguard database servers use SSL, see How do SPP database servers use SSL
- **Verify SSL Certificate**: Use this option to enable or disable SSL Certificate verification on the asset. When enabled, Safeguard for Privileged Passwords compares the signing authority of the certificate presented by the asset to the certificates in the Trusted CA Certificates store every time Safeguard for Privileged Passwords connects to the asset. Trust must be established for Safeguard for Privileged Passwords to manage the asset. For Safeguard for Privileged Passwords to verify an SSL certificate, you must add the asset's signing authority certificate to the Trusted CA Certificates store. Only clear the **Verify SSL Certificate** option if you do not want to establish trust with the

asset.certificate in SPP's Trusted CA Certificates store. One Identity does not recommend disabling this option in production environments.

- **Workstation ID**: Specify the configured workstation ID, if applicable. This option is for IBM i systems.
- **Instance/Service Name**: For SQL Server platforms, specify the **Instance** name if you have configured multiple instances of a SQL Server on this asset. If you have configured a default (unnamed) instance of the SQL Server on the host, you need to provide the IP address and port number.

  For Oracle platforms, use the TNSNAMES naming method to identify the target system in Oracle. Depending on how the Oracle environment is configured, the **Instance** (also called SID in Oracle) and/or the **Service Name** (ServiceName) can be used to identify the target database.

5. Click **OK**.
6. If asked to **Verify Host Authenticity**, click **Yes** to accept the SSH Key for the host.

Add Asset Profile (asset discovery)

During Asset Discovery, SPP automatically adds the assets that it finds and begins to manage them according to the settings in the asset profile you set on the **Rules** tab.

Discovery details

- Once SPP creates an asset, it will not attempt to re-create it or modify the asset if the asset is rediscovered by a different job.
- Any SSH host keys encountered in discovery will be automatically accepted.
- You can configure multiple rules for an Asset Discovery job. When SPP runs the Asset Discovery job, if it finds an asset with more than one rule, it applies the connection and profile settings of the first rule that discovers the asset.

Navigate to:

- web client: **Asset Management** > **Discovery** > **Assets** > (add or edit Asset Discovery job) > **New Asset Discovery Job** dialog > **Asset Discovery Rules** tab > (add asset discovery rule) > **New Asset Discovery Rule** dialog > **Management** tab

To edit the asset profile information

1. On the **Management** tab of the **New Asset Discovery Rule** dialog, next to **Password Profile**, click **Browse**.
2. Select a profile to govern the discovered assets.

   NOTE: You can only choose a profile that is associated with the partition selected in the General tab (asset discovery).

3. Click **Select Password Profile** to save your selection.
4. On the **New Asset Discovery Rule** dialog, next to **SSH Key Profile**, click **Browse**.

5. Select an SSH key profile to govern the discovered assets.

   NOTE: You can only choose a profile that is associated with the partition selected in the General tab (asset discovery).

6. Click **Select SSH Key Profile** to save your selection.
7. On the **New Asset Discovery Rule** dialog, next to **Account Discovery Job**, click **Browse**.
8. Select account discovery job(s) for the discovered assets. Your selection(s) will automatically be saved.

   NOTE: You can only choose a profile that is associated with the partition selected in the General tab (asset discovery).

9. Once your selections have been made, exit the **Select the Account Discovery Job** dialog.
10. On the **New Asset Discovery Rule** dialog, use the **Managed Network** drop-down to select which network to use.

Schedule tab (asset discovery)

Navigate to:

- web client: **Asset Management** > **Discovery** > **Assets** > (add or edit a Asset Discovery job).

On the **Schedule** tab, configure when you want to run the Asset Discovery job.

Select **Run Every** to run the job along per the run details you enter. (If you clear **Run Every**, the schedule details are lost.)

- Select a time frame:
  - **Never**: The job will not run according to a set schedule. You can still manually run the job.
  - **Minutes**: The job runs per the frequency of minutes you specify. For example, `Run Every 30/Minutes` runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
  - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select `Run Every 2/Hours/@ minutes after the hour 15`.
  - **Days**: The job runs on the frequency of days and the time you enter.

    For example, `Run Every 2/Days/Starting @ 11:59:00 PM` runs the job every other evening just before midnight.
  - **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

For example, `Run Every 2/Weeks/Starting @ 5:00:00 AM` and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.

- **Months**: The job runs on the frequency of months at the time and on the day you specify.

  For example, If you select `Run Every 2/Months/Starting @ 1:00:00 AM` along with `Day of Week of Month/First/Saturday`, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click **+ Add** or **— Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter `Run Every 10/Minutes` and set **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

  For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

  For days, enter `Run Every 2/Days` and set **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

Deleting an Asset Discovery job

You can delete an Asset Discovery job.

To delete an asset discovery job

1. Navigate to **Asset Management** > **Discovery**.
2. On the **Assets** tab, select the Asset Discovery job to delete.
3. Click **Delete**.
4. Click **OK**.

Asset Discovery Results

You can view the results of running one or more Asset Discovery jobs.

To view asset discovery results

1. Navigate to **Asset Management** > **Discovery** > **Assets** > **(add or edit a Asset Discovery job)**.
2. On the **Asset Discovery Results** tab:
   - Select the time frame of the completed jobs you want to display which ranges from the last 24 hours to the last 7, 30, 60, or 90 days. Or, click **Custom** to create a custom time frame.
   - Click **Refresh** to refresh the results.
3. Click **Search** and enter the character string to be used to search for a match. For more information, see Search box on page 78.
4. Click a column to sort the column information displayed for each job:
   - **Date/Time**: The most recent date and time the Asset Discovery job successfully ran.
   - **User**: The user who ran the job or **Automated System**, if the job is run on an automated schedule.
   - **Event**: The outcome of running the Asset Discovery job event, which may be **Asset Discovery Succeeded**, **Asset Discovery Failed**, or **Asset Discovery Started**.
   - **Partition**: The partition in which the discovered assets will be managed.
   - **Appliance**: The name of the SPP Appliance.
   - **Directory**: If applicable, the name of the directory on which the Asset Discovery job ran.
   - **# Assets**: The number of asset found during the discovery job; click to view details.

Account Discovery

Account Discovery jobs include the rules SPP uses to perform account discovery against assets. When you add an Account Discovery job, you can identify whether or not to automatically manage found accounts, whether to discover services, and whether to automatically configure dependent systems.

The accounts in the scope of the discovery job may include accounts that were previously added (manually) to the Safeguard partition. For more information, see Adding an account on page 286.

To configure and schedule Account Discovery jobs, perform one of the following:

- You can create or edit an Account Discovery job, then associate assets to the Account Discovery job via the **Occurrences** button.

  IMPORTANT: You must click **Occurrences** to associate assets to the Account Discovery job. If you do not associate the assets to the Account Discovery job, the accounts will not be found.

- You can create or edit an asset and, in the process, assign or create an Account Discovery job. For more information, see Adding an asset.

Supported platforms

SPP supports account discovery on the following platforms:

- AIX
- HP-UX
- Linux / Unix (based)
- MAC OS X
- Solaris
- Starling Connect
- Windows (services and tasks)
- MySQL
- Postgres
- SQL Server
- Oracle
- iDrac
- HP iLO
- HP iLO MP

Properties and toolbar

Go to Account Discovery:

- web client: Navigate to **Asset Management** > **Discovery** > **Accounts**.

Use these toolbar buttons to manage the Account Discovery jobs.

Table 137: Account Discovery: Toolbar

Option	Description
+ New Account Discovery Job	Add an Account Discovery job. For more information, see Adding an Account Discovery job.

Option	Description
Delete	Delete the selected Account Discovery job.
View Details	Modify the selected Account Discovery job. You can also double-click a row to open the edit dialog.
Discover Accounts	Discover the accounts on the selected Account Discovery job. Select the asset on the **Asset** dialog. A **Task** pop-up displays which shows the progress and completion.
Discover Services	Discover the services on the selected Account Discovery job. Select the asset on the **Asset** dialog. A **Task** pop-up displays which shows the progress and completion.
Occurrences	Add, delete, or refresh the assets associated with the Account Discovery job. IMPORTANT: You must associate the assets to the Account Discovery job for the accounts to be found.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of Account Discovery jobs.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 78.

Account Discovery jobs display in the grid.

Table 138: Account Discovery: Account Discovery job grid

Name	Name of the discovery job.
Created By	The creator of the job.
Discovery Type	The type of discovery performed, for example, Windows, Unix, Starling Connect, or Directory.
Directory	The directory on which the discovery job runs.
Partition	The partition in which to manage the discovered assets or accounts.
Schedule	Designates when the discovery job runs.
Discover Services	A check mark displays if the job will discover service accounts.
Auto Configure	A check mark displays if the accounts that are discovered in the Service Discovery job are automatically configured as dependent accounts on the asset.
Assets	Total number of assets assigned to the Account Discovery job. A

	Caution displays if no accounts are assigned to the Account Discovery job therefore no data will be discovered.
Description	The description of the discovery job.

Account Discovery job workflow

SPP's Account Discovery jobs discover accounts of the assets that are in the scope of a profile. Account Discovery jobs can be assigned to multiple assets in the same partition. Account Discovery jobs can include service discovery.

You can configure, schedule, test, and run Account Discovery jobs. After the job has run, you can select whether to manage the account, if it was not identified to be automatically managed.

1. Create an Account Discovery job and associate assets or create an asset and associate the Account Discovery job. For more information, see Adding an Account Discovery job and Adding an asset.
2. Account Discovery jobs can be scheduled to run automatically. In addition, you can manually launch these jobs in any of the following ways:
   - From **Asset Management** > **Discovery** > **Accounts**, click **Discover Accounts** or **Discover Services**.
   - From **Asset Management** > **Assets** > **View Details**, click **Discover Accounts**.
3. After the Account Discovery job runs, you can mark the managed accounts from **Discovery** > **Discovered Items** > **Accounts**:
   - Click **Disable** to prevent SPP from managing the selected account.
   - Click **Enable** to manage the selected account and assign it to the scope of the default profile.

For information about discovery jobs that have run, search the Activity Center. SPP lists the account discovery events in the **Account Discovery Activity** category.

Adding an Account Discovery job

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules that govern how SPP performs account discovery. For more information, see Account Discovery job workflow on page 384.

To add an Account Discovery job

1. Navigate to **Asset Management** > **Discovery** > **Accounts**.
2. Click **+ New Account Discovery Job** to open the **New Account Discovery Job** dialog.

3. On the **General** tab, enter the following information:
   - **Name**: Enter a name for the account discovery job.
   - **Description**: Enter a description of the account discovery job.
   - **Partition**: Use **Browse** to select the partition in which to manage the discovered accounts. You can also add a new partition from the **Select a Partition** dialog (accessed via the **Browse** button) by clicking **+New Partition**.

     IMPORTANT: You cannot change the partition after you save this discovery job.
4. On the **Information** tab, enter the following information:
   - **Discovery Type**: Select the platform (Directory, Role Based, SPS, Starling Connect, Unix, or Windows). Make sure the **Discovery Type** is valid for the assets associated with the partition selected on the **General** tab.
   - **Discover Services**: (For Windows accounts only and deselected by default) Select this check box so that when the discovery job is run, services are discovered.

     If **Discover Services** is selected, the **Automatically Configure Dependent Systems** check box is also available. Select this check box so that any directory accounts that are discovered in the Service Discovery job are automatically configured as dependent accounts on the asset where the service or task was discovered. Once dependencies are found they can only be removed manually from Account Dependencies tab (asset).
5. The **Account Discovery Rules** tab is only available after an account discovery job has been created. For more information, see Adding an Account Discovery rule.
6. On the **Schedule** tab, enter the following information:
   - Select a time frame:
     - **Never**: The job will not run according to a set schedule. You can still manually run the job.
     - **Minutes**: The job runs per the frequency of minutes you specify. For example, `Run Every 30/Minutes` runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
     - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select `Run Every 2/Hours/@ minutes after the hour 15`.
     - **Days**: The job runs on the frequency of days and the time you enter.

       For example, `Run Every 2/Days/Starting @ 11:59:00 PM` runs the job every other evening just before midnight.

- **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

  For example, `Run Every 2/Weeks/Starting @ 5:00:00 AM` and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.

- **Months**: The job runs on the frequency of months at the time and on the day you specify.

  For example, If you select `Run Every 2/Months/Starting @ 1:00:00 AM` along with `Day of Week of Month/First/Saturday`, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click **+ Add** or **— Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter `Run Every 10/Minutes` and set **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

  For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

  For days, enter `Run Every 2/Days` and set **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

7. Click **OK**.

   NOTE: Once you have a saved the new account discovery job, the **Account Discovery Rules** tab will be available and you can add, delete, edit or copy rules. For more information, see Adding an Account Discovery rule on page 387.

8. Select the assets to which the account discovery rule applies using one of these approaches:

   - Go to the asset and configure the account discovery rules. For more information, see Account Discovery tab (add asset) on page 342.
   - From the **Account Discovery** job grid, click the link in the **Asset Count** column to select assets. For more information, see Account Discovery on page 381.

Adding an Account Discovery rule

Use the **Account Discovery Rule** dialog to define the search criteria to be used to discover directory accounts.

You can dynamically tag an account from Active Directory. In addition, you can add a dynamic account group based on membership in an Active Directory group or if the account is in a organizational unit (OU) in Active Directory.

NOTE: For Unix, all search terms return exact matches. A user name search for ADM only returns ADM, not AADMM or 1ADM2. To find all names that contain ADM, you must include "**.***" in the search term; like this: **.*ADM.***.

For Windows and Directory, the search terms is contained in the result. A user name search for ADM returns ADM, AADMM, and 1ADM2.

All search terms are case sensitive. On Windows platforms (which are case insensitive), to find all accounts that start with adm, regardless of case, you must enter **[Aa][Dd][Mm].***.

To add an Account Discovery rule

1. Navigate to **Asset Management** > **Discovery** > **Accounts**.
2. Select an existing account discovery job, and click **View Details**.
3. On the **Account Discovery Rules** tab, click **Edit**.
4. Click **Add** to open the **New Account Discovery Rule** dialog.
5. **Name**: Enter a unique name for the account discovery rule. Limit: 50 characters.
6. **Find By**: Select one of the types of search below.

   If the **Discovery Type** on the previous **Account Discovery** dialog is Windows, Unix, or Role Based; you can search by **Constraints** or **Find All**. The search options **Name**, **Group**, and **LDAP Filter** are only available if the **Discovery Type** is Directory.

   - **Name**: Select this option to search by account name.
     - For a regular search (not directory), in **Contains** enter the characters to search.
     - If you are searching a directory:
       - Select **Start With** or **Contains** and enter the characters used to search subset within the forest.
         When using Active Directory for a search, you can use a full ambiguous name resolution (ANR) search. Type a full or partial account name. You can only enter a single string (full or partial account name) at a time. For example, entering "t" will return all account names that begin with the letter "t": Timothy, Tom, Ted, and so on. But entering "Tim, Tom, Ted" will return no results.

    - Click **Browse** to select the container to search within the directory. The location displays in **Filter Search Location**.
    - Select **Include objects from sub containers** to include sub containers in the search.
    - Click **Preview** then verify the search result in the **Accounts** dialog including **Name** and **Domain Name**.
- **Group**: Select this option to search by group name.
    - Click **+ Add** to launch the **Group** dialog.
    - **Starts with**or **Contains**: Enter a full or partial group name and click **Search**. You can only enter a single string (full or partial group name) at a time.
    - **Filter Search Location**. Click **Browse** to select a container to search within the directory.
    - **Include objects from sub containers**: Select this check box to include child objects.
    - **Select the group to add**: The results of the search displays in this grid. Select one or more groups to add to the discovery job.
    - Click **Preview** then verify the search result in the **Accounts** dialog including **Name** and **Domain Name**.
- **Constraints**: Select this option to search for accounts based on an account's property. All are limited to 255 numeric characters.

  IMPORTANT: Some **Property Constraint** selections may give slow results. Using **Group** is especially discouraged.

  NOTE: Not all constraints will be available for all platforms. For example, while both MySql and Oracle are Role Based discovery types, MySql only supports searching on Permissions while Oracle supports both Roles and Permissions.

    - Selections:
        - **RID (ranges)**: Applies to Windows and Directory (Windows Active Directory). Enter one or more Relative Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separated by a space. For example, type in **1000** followed by a space, then type in **5000-7000**.
        - **GID (ranges)**: Applies to Windows, Directory (Windows Active Directory), and Unix. Enter one or more Group Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separated by a space. For example, type in **8** followed by a space, then type in **10-12**.
        - **UID (ranges)**: Applies to Windows, Directory (Windows Active Directory), and Unix. Enter one or more User

Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separated by a space. For example, type in **1** followed by a space, then type in **5-7**.

- **Name (RegEx)**: Applies to Windows, Directory (Windows Active Directory and LDAP), Unix, and Role Based (MySQL, Postgres, Oracle, SQL Server, Oracle, iDrac, Hp iLO, and HP iLO MP). Using **Name (RegEx)** is discouraged as it may slow your results. It is recommended you use **Name** (described earlier) to search by account name. For an LDAP asset, only substring matching is available (for example, a search term like `abc*`). Matching is case-insensitive. To use, enter a single regular expression pattern. For more information, see Regular expressions on page 688.
- **Group (RegEx)**: Applies to Windows, Directory (Windows Active Directory and LDAP), and Unix. Using **Group (RegEx)** is discouraged as it may slow your results. It is recommended you use **Group** (described earlier) to search by group name. For an LDAP asset, only substring matching is available (for example, a search term like `abc*`). Matching is case-insensitive. To use, enter a single regular expression pattern. For more information, see Regular expressions on page 688.
- **Role (RegEx)**: Applies to Role Based (Oracle and Postgres). Enter one or more roles. For an LDAP asset, only substring matching is available (for example, a search term like `abc*`). Matching is case-insensitive. To use, enter a single regular expression pattern. For more information, see Regular expressions on page 688.
- **Permission (RegEx)**: Applies to Role Based (MySQL, Postgres, Oracle, SQL Server, Oracle, iDrac, Hp iLO, and HP iLO MP). Enter one or more permissions. For an LDAP asset, only substring matching is available (for example, a search term like `abc*`). Matching is case-insensitive. To use, enter a single regular expression pattern. For more information, see Regular expressions on page 688.

- If you are searching a directory:
  - Click **Browse** to select the container to search within the directory. The location displays in **Filter Search Location**.
  - To include sub containers in your search, select **Include objects from sub containers**.
  - Click **Preview** then verify the search result in the **Accounts** dialog including **Name** and **Domain Name**.

7. **Automatically Manage Found Accounts**: Select to automatically add the discovered accounts to SPP. When selected, you can select **Set default password** then enter the password.

8. **Password Sync Group**: Click **Browse** to select a password sync group to control validation and reset across all associated accounts. You can also use **+ Add** to add a new sync group. See: Password sync groups.
9. **Password Profile**: If a profile was not automatically assigned for a sync group (previous step), click **Browse** to select a password profile to identify the configuration settings for the discovered accounts. You can also use **+ New Profile** to add a new password profile. For more information, see Password Profiles tab (partitions) on page 354.
10. **Set default password**: If **Set default password** is selected, the password you enter is a placeholder for the discovered asset until the password is changed for the first time on the asset. If **Set default password** is not selected, no password is stored until the password is changed for the first time on the asset. If the account is requested before the password is changed, an error may result.
    The default password is set in Safeguard for Privileged Passwords but not on the asset.

    > NOTE: If an Account Discovery Rule is configured to set a password, and a password profile (selected via the **Assign to Password Profile** option) is also configured to automatically change passwords, the change password schedule takes precedence and the account will have its password changed upon discovery.

11. **SSH Key Sync Group**: Click **Browse** to select the SSH key sync group. For more information, see SSH Key Sync Groups settings on page 446.
12. **SSH Key Profile**: If a profile was not automatically assigned for a sync group, cFor more information, see SSH Key Profiles tab (partitions) on page 355.
13. **Set default SSH Key**: Select to set a default SSH key. On the **Import an SSH Key** dialog, you can import a private key file for an SSH key that has been generated outside of SPP and assign it to the account. Click **Browse** to import the key file, enter a **Password**, then click **OK**.
    When importing an SSH key that has already been manually configured for an account on an asset, it is recommended that you first verify that the key has been correctly configured before importing the key. For example, you can run an SSH client program to check that the private key can be used to login to the asset: `ssh -i <privatekeyfile> -l <accountname> <assetIp>`. Refer to the OpenSSH server documentation for the target platform for more details on how to configure an authorized key.

    > NOTE:SPP does not currently manage the options for an authorized key. If an imported key has any options configured in the authorized keys file on the asset, these options will not be preserved when the key is rotated by SPP.

14. **Enable Password Request**: This check box is selected by default, indicating that password release requests are enabled for this account. Clear this option to prevent someone from requesting the password for this account. By default, a user can request the password for any account in the scope of the entitlements in which they are an authorized user.
15. **Enable Session Request**: This check box is selected by default, indicating that session access requests are enabled for this account. Clear this option to prevent

someone from requesting session access using this account. By default, a user can make an access request for any account in the scope of the entitlements in which they are an authorized user.

16. **Enable SSH Key Request**: This check box is selected by default, indicating that SSH key release requests are enabled for this account. Clear this option to prevent someone from requesting the SSH key for this account. By default, a user can request the SSH key for any account in the scope of the entitlements in which they are an authorized user.
17. **Enable API Key Request**: This check box is selected by default, indicating that API key release requests are enabled for this account. Clear this option to prevent someone from requesting the API key for this account. By default, a user can request the API key for any account in the scope of the entitlements in which they are an authorized user.
18. (For directory accounts only) **Available for use across all partitions (Global Access)**: When selected, any partition can use this account and the password is given to other administrators. For example, this account can be used as a dependent account or a service account for other assets. Potentially, you may have assets that are running services as the account, and you can update those assets when the service account changes. If not selected, partition owners and other partitions will not know the account exists. Although archive servers are not bound by partitions, this option must be selected for the directory account for the archive server to be configured with the directory account.
19. **Tags**: This tab allows you to select tags or add new tags with rules.
20. Click **Apply**.
21. Click **OK** to save the Account Discovery job.

Deleting an Account Discovery job

You can delete an Asset Discovery job.

To delete an Account Discovery job

1. Navigate to **Asset Management** > **Discovery** > **Accounts**.
2. Select an Account Discovery job.
3. Click **Delete** to delete the selected Account Discovery job.
4. Click **Yes**.

Account Discovery Results

You can view the results of running one or more Account Discovery jobs. To see the results of discoveries, see Discovered Accounts

To view Account Discovery results

1. Navigate to **Asset Management** > **Discovery** > **Accounts** (add or edit a Account Discovery job).
2. On the **Account Discovery Results** tab:
   - Select the time frame of the completed jobs you want to display which ranges from the last 24 hours to the last 7, 30, 60, or 90 days. Or, click **Custom** to create a custom time frame.
   - Click **Refresh** to refresh the results.
3. View the following information displays for each job:
   - **Date/Time**: The most recent date the Account Discovery job successfully ran.
   - **User**: The user who ran the job or **Automated System**, if the job is run on an automated schedule.
   - **Event**: The outcome of running the Account Discovery job event, which may be **Account Discovery Succeeded**, **Account Discovery Failed**, or **Account Discovery Started**.
   - **Asset**: The asset which is associated with the Account Discovery job.
   - **Partition**: The partition in which the discovered accounts will be managed.
   - **Profile**: The profile which will govern the discovered accounts.
   - **Appliance**: The name of the Safeguard for Privileged Passwords Appliance.
   - **# Accounts**: The number of accounts found during the discovery job; click to view details.

Discovered Accounts

You can view the results of all Account Discovery jobs that have ever run in a partition (in other words, all accounts ever discovered) and choose to enable or disable the accounts.

Accounts created display as managed accounts in the Discovered Accounts properties grid (see below). For more information, see .

Go to Discovered Accounts:

- web client: Navigate to **Asset Management** > **Discovery** > **Discovered Items** > **Accounts** tile.

Use these toolbar buttons to manage the discovered accounts.

Table 139: Discovery: Discovered Accounts toolbar

Option	Description
Manage	Click **Manage** to change the status to managed for one or

Option	Description
	more selected accounts. Accounts that are managed by SPP will be added to the asset's list of accounts and access request policies. The Discovery job may mark the accounts managed, or they can be selected and marked managed using this button.
Ignore	Click **Ignore** to set the **Status** to **Ignore** to prevent Safeguard for Privileged Passwords from managing the selected account. If the status of the account is **None** then the resulting status will be **Ignored**. If the status of the account is **Managed** then you will need to use the **Accounts** page to change the status.
Show Ignored	Display the accounts with a **Status** of **Ignored**.
Hide Ignored	Hide the accounts with a **Status** of **Ignored**.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Retrieve and display an updated list of discovered accounts. Ignored accounts are not displayed if **Hide Ignored** is selected.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 78.

The following information displays.

Table 140: Discovery: Discovered Accounts properties grid

Property	Description
Status	The discovered account may be: • **Managed**: A discovered account that is managed. • **None**: A discovered account that was not auto managed when discovered. • **Ignored**: A discovered account that was not auto managed and was ignored from discovery. • **Disabled**: A discovered account that previously had the status of Managed and then was marked Ignored. A disabled account is not removed from the Asset account list nor unconfigured as a dependent account. It is marked disabled and cannot be used or acted upon.
Name	The name of the account in Safeguard that maps to the discovered account associated with the asset. This can be a local account or an Active Directory account

Property	Description
Domain Name	The domain name of the account if the account is an Active Directory account.
Asset Name	The name of the asset the account was discovered on.
Account Discovery Job	Name of the discovery schedule.
Asset Discovery Rule	The name of the Asset Discovery rule applied that discovered the account.
Date/Time Discovered	The date and time when the service or task was discovered.

Service Discovery Results

Setting up Service Discovery

To discover Windows services, you must first create an Account Discovery job, including an Account Discovery Rule, and select **Discover Services**. When the discovery job is run, services are discovered. The discovery of services is not dependent on the discovery rules. For more information, see Adding an Account Discovery job.

To view Service Discovery results

1. Navigate to **Asset Management** > **Discovery** > **Accounts** > (add or edit a Account Discovery job).
2. On the **Service Discovery Results** tab:
   - Select the time frame of the completed jobs you want to display which ranges from the last 24 hours to the last 7, 30, 60, or 90 days. Or, click **Custom** to create a custom time frame.
   - Click **Refresh** to refresh the results.
3. Click **Search** and enter the character string to be used to search for a match. For more information, see Search box on page 78.
4. View the following information displays for each job:
   - **Date/Time**: The most recent date the Account Discovery job successfully ran.
   - **User**: The user who ran the job or **Automated System**, if the job is run on an automated schedule.
   - **Event**: The outcome of running the discovery job event, which may be **Service Discovery Started**, **Service Discovery Succeeded**, or **Service Discovery Failed**. Succeeded and failed appear in **Event** on the **Service Discovery Results** dialog. All three events display in the Activity Center.
   - **Asset**: The asset that is associated with the discovery job.

- **Partition**: The partition in which the discovered service accounts will be managed.
- **Profile**: The profile that will govern the discovered service accounts.
- **Appliance**: The name of the Safeguard for Privileged Passwords Appliance.
- **# Services**: The number of service accounts found during the discovery job.

Discovered Services

The **Discovered Services** tile displays information for the selected partition on which the services were discovered.

The Asset Administrator or delegated administrator can configure service discovery jobs to scan Windows assets and discover Windows services that may require authorization credentials.

The following types of services are discovered on managed Windows assets:

- Windows services
- Scheduled tasks
- IIS Application Pools
- Com+ applications

If the Windows asset is joined to a Windows domain, the authorization credentials can be local on the Windows asset or be Active Directory credentials.

IMPORTANT: For Windows SSH assets, a local account does not have the access necessary to discover services running as domain accounts. So if a local account is used as the service account for a Windows SSH asset, Safeguard for Privileged Passwords will only discover services running as local accounts on that asset and domain account dependencies will not be updated.

IMPORTANT: If your asset's management type is Windows (either desktop or server) then in order to discover IIS App Pools using Service Discovery, you will need to install one of the following features under the Management Tools section of the Web Server role:

- IIS 6 Metabase Compatibility and IIS 6 WMI Compatibility (for more information, see Metabase Compatibility with IIS 7 and Above)
- IIS Management Scripts and Tools (for more information, see Managing Applications and Application Pools on IIS 7.0 with WMI)

NOTE: Discovery is supported for each of these service types on Windows Server, Windows RM, and Windows SSH platforms; but the Windows Server platform does not support updating account dependencies on IIS App pools and Com+ applications.

Running Service Discovery jobs automatically and manually

- Service discovery jobs run automatically in the background if **Discover Services** check box is selected. If the **Automatically Configure Dependent Systems** check

box is selected, any directory accounts that are discovered in the Service Discovery job are automatically configured as dependent accounts on the asset where the service was discovered. For more information, see Adding an Account Discovery job.

- You can manually run a Service Discovery job from **Asset Management** > **Assets** > **Discovered Services**. For more information, see Discovered Services tab (asset) on page 312.

Discovered services and tasks association to known Safeguard accounts

Service discovery jobs associate Windows services with accounts that are already managed by Safeguard for Privileged Passwords. The accounts put under management display with an **Account Status** of **Managed**.

Service Discovery with Active Directory

A discovered service configured to run as an Active Directory account can be automatically associated to the asset with the account managed by Safeguard. Effectively, the asset will have an account dependency on the account.

To automatically associate, the Account Discovery job (which runs when Safeguard synchronizes the directory) must have the **Automatically Manage Found Accounts** check box selected. For more information, see Adding an Account Discovery rule on page 387. Once configured as an account dependency, when the Active Directory account's password is changed by Safeguard, Safeguard updates the password for the service on the asset, according to the asset's profile change settings. For more information, see Adding change password settings.

View Service Discovery job status

From the Activity Center, you can select the Activity Category named Service Discovery Activity, which shows the Event outcomes: **Service Discovery Succeeded**, **Service Discovery Failed**, or **Service Discovery Started**.

Discovered Services toolbar and properties

Go to Discovered Services:

- web client: Navigate to **Asset Management** > **Discovery** > **Discovered Items** > **Services** tile.

Use these toolbar buttons to manage the discovered services.

Table 141: Discovery: Discovered Services toolbar

Option	Description
Show > **Ignore**	The **Show** and **Ignore** buttons control the **Service Ignored** column on this window so the administrator can either display or ignore the rows. The **Account Status** column is controlled by the **Manage** and **Ignore** buttons on the **Discovered Accounts** grid. For more information, see Discovered Accounts on page 392.

Option	Description
Show Ignored	Display the accounts with a **Status** of **Ignored**.
Hide Ignored	Hide the accounts with a **Status** of **Ignored**.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Retrieve and display an updated list of discovered accounts. Ignored accounts are not displayed if **Hide Ignored** is selected.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 78.

The grid shows the **Asset Name**, **Account**, **Domain Name**, **System Name**, and **Account Status** for the **Discovered Account** that Safeguard found that is matched up with the service discovered. The service is identified by a **Service Name** (with a **Service Type** of **Service**, **IIS App pool**, **Com+ service**, or **Task**).

Table 142: Discovery: Discovered Services properties

Property	Description
Asset Name	The name of the asset where the service was discovered.
Account	The name of the account that maps to the **Discovered Account** column.
Domain Name	The domain name of the account if the account is an Active Directory account. Used to help determine uniqueness. Only Active Directory accounts can be configured as dependent accounts.
System Name	The system or asset that hosts the discovered mapped account.
Account Status	The **Account Status** column is controlled by the **Manage** and **Ignore** buttons on the **Discovered Accounts** grid. For more information, see Discovered Accounts on page 392. The discovered account may be: • **Managed**: A discovered account that is managed. • **None**: A discovered account that was not auto managed when discovered. • **Ignored**: A discovered account that was not auto managed and was ignored from discovery. • **Disabled**: A discovered account that previously had the status of Managed and then was marked Ignored. A disabled account is not removed from the Asset account list nor unconfigured as a dependent account. It is marked disabled and cannot be used or acted upon.

Property	Description
Dependent Account	A ✔ check displays if the account is associated as an account dependency on the asset. The value is blank if the account is not associated as an account dependency of the asset. This automatic dependency mapping only happens if the **Automatically Manage Found Accounts** option is selected on the Account Discovery job associated with the profile that is associated to the asset. For more information, see Adding an Account Discovery job.
Service Type	Type of service discovered. Values may be **Service**, **IIS App pool**, **Com+ service**, or **Task**.
Service Name	The name of the discovered service.
Service Enabled	A ✔ check displays if the service on the asset is enabled on the target machine. If there is no check mark, the service is disabled on the target machine.
Service Ignored	Ignored means the service will not show up in the grid. In other words, the service is hidden. This is controlled by the ▣ **Show** > ⊘**Ignore** actions on this grid.
Discovered Account	The discovered account name. If the account has an **Account Status** of **Managed**, then the **Account**, **Domain Name**, and **System Name** display.
Date/Time Discovered	The date and time when the service was discovered.

SSH Key Discovery

You can schedule one or more SSH Key Discovery jobs to run automatically against the accounts you have added to SPP (SPP). The SSH keys in the scope of the discovery job may include SSH keys that were previously added (manually) to the SPP partition.

For more information, see Discover SSH Key settings on page 444.

When an SSH Key Discovery job runs, the found SSH keys are listed in the Discovered SSH Keys tile in the selected partition. They are also shown in Assets (under the Discovered SSH Keys tab) and in Accounts (under the Discovered SSH Keys tab).

Supported platforms

SSH Key Discovery is supported on the following platforms:

- Hardware/Custom (A custom script is required to accommodate how keys are handled.)

- Drac
- Fortinet
- Junos
- PanOs
- Window OS
- General Unix style platforms
    - Linux
    - Aix
    - Hpux
    - Solaris
    - F5BigIP
    - FreeBSD
    - MacOS

Properties and toolbar

Go to SSH Key Discovery:

- web client: Navigate to **Asset Management** > **Discovery** > **SSH Keys**.

Use these toolbar buttons to manage the SSH Key Discovery jobs.

Table 143: SSH Key Discovery: Toolbar

Option	Description
New SSH Key Discovery Job	Add an SSH Key Discovery job. For more information, see Adding an SSH Key Discovery job on page 401.
Delete	Delete the selected SSH Key Discovery job.
View Details	Modify the selected SSH Key Discovery job. You can also double-click a row to open the edit dialog.
Discover SSH Keys	Click this button to open a new window where you can select a single account to run the selected SSH Key Discovery job on.
Occurrences	View the accounts associated with the selected discover SSH key settings by account **Name** and **Asset Name**. The **Inherited** column has a check mark if the assignment is an inherited association via the asset. If not inherited, the accounts have an explicit assignment to a Profile/SSH Key Discovery job. For more information, see About profiles on page 346.

Option	Description
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of SSH Key Discovery jobs.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 78.

SSH Key Discovery jobs display in the grid.

Table 144: SSH Key Discovery: SSH Key Discovery job grid

Name	Name of the SSH Key Discovery job.
Created By	Indicates the creator of the SSH Key Discovery job.
Partition	The partition in which to manage the discovered SSH keys.
Schedule	Designates when the SSH Key Discovery job runs.
Profiles	Lists the number of profiles that are configured with this job. Click the link to go to the **SSH Key Profiles** dialog that lists the **Name** and **Description** of the SSH key profiles that are associated with this SSH key discovery job.
Accounts	Lists the number of accounts that are associated with this SSH key discovery job via profile association. Click the link to view the account **Name** and parent **System Name** of this SSH key discovery job.
Description	The description of the SSH Key Discovery job.

SSH Key Discovery job workflow

The SSH Key Discovery jobs discover SSH keys of the accounts that are in the scope of the profile. You can configure, schedule, and run SSH Key Discovery jobs. After a job has run, you can view the Discovered SSH Keys under the tab of that name. You will see the following: Key Fingerprint, Comment (that is in the key), Key Type, Key Length, Asset Name, Account Name, and Account Status ("managed" means SPP manages the account, and "disabled" means SPP does not manage the account).

1. Set up the partition with the SSH key profile. For more information, see SSH Key Profiles tab (partitions) on page 355.
2. Create an SSH Key Discovery job. For more information, see Adding an SSH Key Discovery job on page 401.
3. SSH Key Discovery jobs can be scheduled to run automatically. In addition you can manually launch a job on a single account:

- From **Asset Management** > **Discovery** > **SSH Keys** select the SSH Key Discovery job to run, then click **Discover SSH Keys**.

4. After the SSH Key Discovery job runs, click SSH Key Discovery Results tile to view the SSH Keys found. For more information, see SSH Key Discovery Results on page 402.

   NOTE: The discovery job finds all current SSH keys that match the discovery rule's criteria. SSH Key Discovery does not update existing accounts.

Search the Activity Center for information about discovery jobs that have run. SPP lists the SSH Key Discovery events in the **SSH Key Discovery Activity** category. For more information, see Activity Center on page 564.

Adding an SSH Key Discovery job

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules that govern how SPP performs SSH key discovery. For more information, see SSH Key Discovery job workflow on page 400.

To add an SSH Key Discovery job

1. Navigate to **Asset Management** > **Discovery** > **SSH Keys**.
2. Click **+ New SSH Key Discovery Job** to open the **New SSH Key Discovery Job** dialog.
3. Provide the following:
   a. **Name**: Enter a name for the account discovery job. Limit: 50 characters.
   b. **Description**: Enter descriptive text about the SSH Key Discovery job. Limit: 255 characters
   c. **Partition**: **Browse** to select a partition.
   d. To identify when to **Discover SSH Key**, on the **Schedule** tab:
      - Select a time frame:
        - **Never**: The job will not run according to a set schedule. You can still manually run the job.
        - **Minutes**: The job runs per the frequency of minutes you specify. For example, **`Run Every 30/Minutes`** runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
        - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select **`Run Every 2/Hours/@ minutes after the hour 15`**.
        - **Days**: The job runs on the frequency of days and the time you enter.

For example, `Run Every 2/Days/Starting @ 11:59:00 PM` runs the job every other evening just before midnight.

- **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

  For example, `Run Every 2/Weeks/Starting @ 5:00:00 AM` and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.

- **Months**: The job runs on the frequency of months at the time and on the day you specify.

  For example, If you select `Run Every 2/Months/Starting @ 1:00:00 AM` along with `Day of Week of Month/First/Saturday`, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time.

  You can click **+ Add** or **— Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter `Run Every 10/Minutes` and set **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

  For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

  For days, enter `Run Every 2/Days` and set **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

4. To save and close , click **OK**.

SSH Key Discovery Results

You can view the results of running one or more SSH Key Discovery jobs. To see the results of discoveries, see Discovered SSH Keys

To view SSH Key Discovery Results

1. Navigate to **Asset Management** > **Discovery** > **SSH Keys** > (add or edit an SSH Key Discovery job).
2. On the **SSH Key Discovery Results** tab:
   - Select the time frame of the completed jobs you want to display which ranges from the last 24 hours to the last 7, 30, 60, or 90 days. Or, click **Custom** to create a custom time frame.
   - Click **Refresh** to refresh the results.
3. To display what you want in the grid, click **Search** and enter the character string to be used to search for a match. For more information, see Search box on page 78.
4. View the following information displays for each job:
   - **Date/Time**: The most recent date the SSH Key Discovery job successfully ran.
   - **User**: The user who ran the job or **Automated System**, if the job is run on an automated schedule.
   - **Event**: The outcome of running the SSH Key Discovery job event, which may be **SSH Key Discovery Succeeded**, **SSH Key Discovery Failed**, or **SSH Key Discovery Started**.
   - **Account**: The account which is associated with the SSH Key Discovery job .
   - **Asset**: The asset which is associated with the SSH Key Discovery job.
   - **Partition**: The partition in which the discovered SSH keys will be managed.
   - **SSH Key Profile**: The profile which will govern the discovered SSH keys.
   - **Appliance**: The name of the Safeguard for Privileged Passwords Appliance.
   - **# SSH Keys**: The number of SSH Keys found during the discovery job; click the displayed number to view the list of SSH Keys found on the account.

Discovered SSH Keys

You can view the current SSH Key Discovery results for a selected partition. The number of discovered keys for an account will reflect the number of SSH keys discovered in the account's authorized keys file.

SSH keys currently in use by an account will have a check mark in the SSH Key Managed column in the Discovered SSH Keys properties grid (see below).

Go to Discovered SSH Keys:

- web client: Navigate to **Asset Management** > **Discovery** > **Discovered Items** > **SSH Keys** tile.

Select the partition for which you want to see the SSH Key results.

Use these toolbar buttons to manage the discovered accounts.

Table 145: Discovery: Discovered SSH Keys toolbar

Option	Description
Revoke	Use this button to revoke access for unmanaged SSH keys.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Retrieve and display an updated list of discovered SSH keys. If SSH Keys are deleted from the account's authorized keys file, they will be removed from the discovered list when the discovery job runs.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 78.

The following information displays.

Table 146: Discovery: Discovered SSH Keys properties grid

Property	Description
Fingerprint	The fingerprint of the SSH key used for authentication.
Account Status	The status of the account where the SSH key was discovered.
SSH Key Managed	This column will have a check mark indicating the SSH key currently in use on the account.
Comment	Free form comment included in the SSH key.
Key Type	The SSH authentication key type, such as RSA and DSA. For more information, see SSH Key Profiles on page 433.
Key Length	The supported RSA or DSA key length displays. For more information, see SSH Key Profiles on page 433.
Asset Name	The name of the asset where the SSH key was discovered.
Account	The name of the account where the SSH key was discovered.
Date/Time Discovered	The date and time when the SSH key was discovered.

Profiles

Within the web client, the **Profiles** page displays information on the currently configured profiles in use by SPP.

To access **Profiles**:

- web client: Navigate to **Asset Management** > **Profiles**.

The Profiles page is separated into sections:

- Password Profiles (profiles)Password Profiles (profiles)
- SSH Key Profiles (profiles)

Password Profiles (profiles)

Within the web client, the **Password Profiles** tab on the **Profiles** page displays information on the currently configured password profiles in use by SPP.

To access the **Password Profiles** tab on the **Profiles** page:

- web client: Navigate to **Asset Management** > **Profiles** which by default displays the **Password Profiles** tab. If needed, you can use the partition drop-down to select the parent partition of the profile (by default all profiles are displayed).

  Select a profile, then click to display additional information and options.

Selecting one of the profiles displays the following information:

- Properties tab (profiles): Displays general information about the selected profile.
- Assets tab (profiles): Displays the assets assigned to the selected profile.
- Accounts tab (profiles): Displays the accounts assigned to the selected profile.

Toolbar

Use these toolbar buttons to manage profiles:

- **New Profile**: Add profiles to SPP.
- **Delete**: Remove the selected profile.
- **View Details**: Select a profile then click this button to open additional information and options for the profile.
- **Set as Default**: Select a profile then click this button to set it as the default profile.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of profiles.

When the **Password Profiles** tab on the **Profiles** page is selected, a **View Password Profile Components** link is available. For more information, see View Password Profile Components (profiles).

Properties tab (profiles)

The **Properties** tab lists information about the selected profile.

To access the **Properties** tab, in the web client, navigate to **Asset Management** > **Profiles** > ✎ **View Details** > **Properties**.

The following fields are displayed based on the type of profile:

Table 147: Properties tab: General properties

Property	Description
Name	The profile's name.
Description	Description of the profile.
Partition	The name of the partition where the selected profile resides.
🗑 **Delete**	Click this button to delete the selected profile.

The following information is also available on the **Properties** tab:

Table 148: Properties tab: Check Password properties

Property	Description
Check Password Settings	Name of the check password rule.
Description	Description of the check password rule.
Schedule	The schedule of the check password rule.

Table 149: Properties tab: Change Password properties

Property	Description
Change Password Settings	Name of the change password rule.
Description	Description of the change password rule.
Schedule	The schedule of the change password rule.

Table 150: Properties tab: Account Password Rule properties

Property	Description
Account Password Rule	Name of the account password rule.
Rule Summary	Summary of the account password rule.

Table 151: Properties tab: Password Sync Groups properties

Property	Description
Enabled	If **Enabled** is selected, the sync runs with the profile change schedule.
Status	The ✓ **Status** displays if all account passwords are in sync with the password sync group. The **Status** is ⚠ if any password for any account within the sync group does not match the common password.
Name	The name of the password sync group.
Accounts	The number of accounts to synchronize with a common password.
Next Sync	The date the sync group password will be synchronized across all accounts.
Description	Information about the rule.

🗑 **Delete**: Click this button to delete the selected profile.

Assets tab (profiles)

The **Assets** tab displays the assets assigned to the selected profile.

Click + **Add Asset** from the details toolbar to add one or more assets to the selected profile.

To access **Assets**:

- web client: Navigate to **Asset Management** > **Profiles** > **Password Profiles** > (View Details) > **Assets**.

Table 152: Profiles: Assets tab properties

Property	Description
Name	The asset name.
Platform	The platform of the selected asset.
Disabled	A check in this column indicates the asset is disabled.
Product License	If applicable (for example, for a Windows asset), indicates your license model, such as System or Desktop.
Description	Descriptive information entered when the asset was added.
Tags	The tags associated with the asset.

Use these buttons on the details toolbar to manage the assets assigned to the selected partition.

Table 153: Profiles: Assets tab toolbar

Option	Description
Add Asset	Add an asset to the profile.
Remove	Remove the selected asset.
View Details	After selecting an asset from the table, click this button to view additional details and configuration options.
Access Request	Allows you to enable or disable access request services for the selected asset. Menu options include **Enable Session Request** and **Disable Session Request**.
SSH Host Key	This drop-down contains the following options depending on the status of the SSH Host Key: • Retrieve SSH Host Key • Discover SSH Host Key • Set SSH Host Key • Download SSH Host Key
Test Connection	Verify that SPP can log in to the asset using the service account credentials that you have provided.
Syncronize Now	Run the directory addition (incremental) synchronization process by asset and account. The sync is queued by asset by provider and runs one directory sync on that asset at a time. You can run multiple syncs in parallel on different assets. This is the faster type of directory sync because deletions are not synced. A **Tasks** window displays the progress and outcome of the task. You can click **Details** to see more information or click **Stop** to cancel the task. In addition, this process runs through the discovery, if there are discovery rules and configurations set up.The API (`Assets/Synchronize`) can be used to run the deletion (full) sync which includes all deletions, additions, and changes. This sync takes longer (perhaps hours), especially the first time it is run based on your directory setup.
Discover Accounts	Run the associated Account Discovery job. For more information, see Account Discovery on page 381.
Enable-Disable	Select one of the following:

Option	Description
	Select ▣ **Enable** to have SPP manage a disabled asset. Account Discovery jobs find all accounts that match the discovery rule's criteria regardless of whether it has been marked **Enabled** or **Disabled** in the past. Select ⊘ **Disable** to prevent SPP from managing the selected asset. When you disable an asset, SPP disables it and removes all associated accounts. If you choose to manage the asset later, SPP re-enables all the associated accounts.
Show Disabled	Display the assets that are not managed and are disabled and have no associated accounts. Asset management can be controlled by selecting an asset and clicking **Enable-Disable**.
Hide Disabled	Hide the assets that are not managed and are disabled and have no associated accounts. Asset management can be controlled by selecting an asset and clicking **Enable-Disable**.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Retrieve and display an updated list of assets associated with the selected partition.
Search	To locate a specific asset in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Accounts tab (profiles)

A profile's **Accounts** tab displays the accounts associated with this profile.

Click **+Add Account**/**New Account** from the details toolbar to associate an account with the selected profile.

To access **Accounts**:

- web client: Navigate to **Asset Management** > **Profiles** > **Password Profiles** > (View Details) > **Accounts**.

Table 154: Profiles: Accounts tab properties

Property	Description
Name	Name of an account associated with the selected asset.

Property	Description
	While you can associate an account with only one asset, you can log in to an asset with more than one account.
Domain Name	The domain name for the account and helps to determine the uniqueness of accounts.
Parent	The name of the object to which the selected account is a child.
Password Profile	The name of the password profile.
SSH Key Profile	The name of the SSH key profile.
Service Account	A ✔ check in this column indicates that the account is a service account.
Password Request	A ✔ check in this column indicates that password release requests are enabled for the account. Click **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected account.
Session Request	A ✔ check in this column indicates that session access requests are enabled for the account. Click **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected account.
SSH Key Request	A ✔ check in this column indicates that SSH key release requests are enabled for the account. Click **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected account.
Disabled	A ✔ check in this column indicates that the asset is not managed, is disabled, and has no associated accounts.
Password	A ✔ check in this column indicates a password is set for the account. For more information, see Checking, changing, or setting an account password on page 291.
TOTP Authenticator	A ✔ check in this column indicates a TOTP Authenticator is set for the account. For more information, see Setting a TOTP authenticator.
SSH Key	A ✔ check in this column indicates an SSH key is set for the account. For more information, see Checking, changing, or setting an SSH key on page 292.
API Keys	A ✔ check in this column indicates an API key is set for the account. For more information, see Checking, changing, or setting

Property	Description
	an SSH key on page 292.
Description	Descriptive information entered when the account was added.
Tags	Tags associated with the account.

Use these buttons on the details toolbar to manage your asset accounts.

Table 155: Profiles: Accounts tab toolbar

Option	Description
Add Account	Add an account to the profile.
Remove	Remove the selected account from the asset.
View Details	After selecting an account from the table, click this button to view additional details and configuration options.
Account Secrets	Menu options include: • **Check Password** • **Change Password** • **Check SSH Key** • **Change SSH Key**
Access Request	Select an option to enable or disable access request services for the selected account. Values are derived from whether the platform of the asset indicates it supports any of the following: Password Request, SSH Key Request, Session Request. You can enable or disable Password Request, Session Request, and SSH Key Request, as needed. Service Accounts are created when the Asset is created and by default are not enabled for session or password access. Discovered Accounts are controlled by the Account Discovery template that is used in discovering the accounts. They are a property of the rule template of the Account Discovery job. For more information, see Adding an Account Discovery rule on page 387.
Enable-Disable	Select one of the following: Select **Enable** to have Safeguard for Privileged Passwords manage a disabled account. Select **Disable** to prevent Safeguard for Privileged Passwords from managing the selected account.

Option	Description
Show Disabled	Display the accounts that are not managed and are disabled.
Hide Disabled	Hide the accounts that are not managed and are disabled..
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of asset accounts.
Search	To locate a specific asset account or set of accounts in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

View Password Profile Components (profiles)

When the **Password Profiles** tab on the **Profiles** page is selected, a **View Password Profile Components** link is available. This link displays information on the currently configured password profile components in use by SPP.

To open the **View Password Profile Components** link on the **Profiles** page:

- web client: Navigate to **Asset Management** > **Profiles** > **Password Profiles** and click the **View Password Profile Components** link.

The **View Password Profile Components** view contains the following tabs:

- **Check Password**: This tab provides information on the currently configured check password schedules. You can use the **Refresh** button to update the listed schedules.
- **Change Password**: This tab provides information on the currently configured change password schedules. You can use the **Refresh** button to update the listed schedules.
- **Account Password Rules**: This tab provides information on the currently configured account password rules. You can use the **Refresh** button to update the listed rules.
- **Password Sync Groups**: This tab provides information on the currently configured password sync groups. From this tab the following options are available:
  - **Add**: Add a new password sync group.
  - **Delete**: Remove the selected password sync group.
  - **View Details**: View additional information for the selected password sync group.

- **Enable-Disable**: Use these buttons to either enable or disable the password sync group.
- **Change Sync Group Password**:
- **Refresh**: Update the listed password sync groups.

Managing password profiles

Use the controls and tabbed pages on the **Profiles** page to perform the following tasks to manage password profiles:

- Adding a password profile
- Password Profiles
- Setting a default password profile
- Deleting a password profile

Adding a password profile

It is the responsibility of the Asset Administrator to add partitions to SPP.

To add a password profile

1. Navigate to **Asset Management** > **Profiles** > **Password Profiles**.
2. Click + **New Profile** from the toolbar.
3. In the **General** dialog, enter the following information:
   a. **Name**: Enter a unique name for the profile. Limit: 50 characters.
   b. **Description**: (Optional) Enter information about this profile. Limit: 255 characters.
4. On the **Check Password** tab, select a previously defined check password setting from the drop-down menu or click + **Add** to add a new check password setting. These are the rules used to verify account passwords. For more information, see Adding check password settings on page 415.
5. On the **Change Password** tab, select a previously defined change password setting from the drop-down menu or click + **Add** to add a new change password setting. These are the rules used to reset account passwords. For more information, see Adding change password settings on page 418.
6. On the **Account Password Rule** tab, select a previously defined account password rule or click + **Add** to add a new account password rule. An account password rule is a complexity rule that governs the construction of the new password created by SPP

during an automatic password change. For more information, see Adding an account password rule on page 425.

7. Click **OK** to save the password profile.
8. When creating a new profile, the **Password Sync Groups** tab is not available. This tab is displayed while editing a profile. You can use the **Password Sync Groups** tab to add or update a password sync group governed by the profile change schedule. For more information, see Password sync groups on page 427.

Password Profiles

Use **Password Profiles** to define the profile configuration settings, including account password rules and password check and change schedules, which can then be used in profile definitions.

Navigate to **Asset Management** > **Profiles** > **Password Profiles**.

Table 156: Profile settings

Setting	Description
Account Password Rules	Where you define the complexity rules used by SPP when constructing new passwords during an automatic account password change
Change Password	Where you define the rules SPP uses to reset account passwords
Check Password	Where you define the rules SPP uses to verify account passwords
Password sync groups	Where you define the password sync groups and associated accounts so SPP can synchronize passwords across accounts

Check Password

Check password settings are the rules SPP uses to verify account passwords.

Navigate to **Asset Management** > **Profiles** > **View Password Profile Components** > **Check Password**.

The **Check Password** pane displays the following about the listed check password setting rules.

Table 157: Check Password: Properties

Property	Description
Name	The name of the check password rule.
Partition	The partition that uses the rule.
Description	Information about the rule.
Schedule	Displays the selected rule's schedule.

Use these toolbar buttons to manage the check password setting rules.

Table 158: Check Password: Toolbar

Option	Description
Add	Add a check password rule. For more information, see Adding check password settings on page 415.
Delete	Remove the selected rule.
Edit	Modify the selected rule.
Refresh	Update the list of check password rules.
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding check password settings

It is the responsibility of the Asset Administrator or the partition's delegated administrator to define the rules SPP uses to verify account passwords.

Navigate to **Asset Management** > **Profiles** > **View Password Profile Components** > **Check Password**.

To add a password validation schedule

1. Click **+Add** to open the **Check Password Settings** dialog.
2. Enter a **Name** of up to 50 characters for the rule.
3. Enter a **Description** of up to 255 characters for the rule.
4. Select the partition using the browse button.
5. Optionally, complete either of these settings:
   - **Reset Password on Mismatch**: Select this option to automatically change a password when SPP detects the password in the appliance database differs from the password on the asset.
   - **Notify Owners on Mismatch**: Select this option to trigger a notification when SPP detects a password mismatch.

     NOTE: To send event notifications to a user, you must configure SPP to send alerts. For more information, see Configuring alerts on page 95. Set up an email template for the Password Check Mismatch event type.
6. Open the **Schedule** tab and choose an interval.
7. In the **Schedule** dialog, select **Run Every** to run the job along per the run details you enter. (If you deselect **Run Every**, the schedule details are lost.)

- Configure the following.

  To specify the frequency without start and end times, select from the following controls. If you want to specify start and end times, go to the **Use Time Window** selection in this section.

  Enter a frequency for **Run Every**. Then, select a time frame:

  - **Minutes**: The job runs per the frequency of minutes you specify. For example, **Every 30 Minutes** runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
  - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select **Runs Every 2 Hours @ 15 minutes after the hour**.
  - **Days**: The job runs on the frequency of days and the time you enter.

    For example, **Every 2 Days Starting @ 11:59:00 PM** runs the job every other evening just before midnight.
  - **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

    For example, **Every 2 Weeks Starting @ 5:00:00 AM** and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.
  - **Months**: The job runs on the frequency of months at the time and on the day you specify.

    For example, If you select **Every 2 Months Starting @ 1:00:00 AM** along with **First Saturday of the month**, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click + **Add** or − **Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter **Every 10 Minutes** and **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

  For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

For days, enter **Every 2 Days** and set the **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

- **(UTC) Coordinated Universal Time** is the default time zone. Select a new time zone, if desired.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

Change Password

Change password settings are the rules SPP uses to reset account passwords.

Navigate to **Asset Management** > **Profiles** > **View Password Profile Components** > **Change Password**.

The **Change Password** pane displays the following about the listed change password setting rules.

Table 159: Change Password: Properties

Property	Description
Name	The name of the rule.
Partition	The partition that uses the rule.
Description	Information about the rule.
Schedule	Displays the selected rule's schedule.

Use these toolbar buttons to manage the change password setting rules.

Table 160: Change Password: Toolbar

Option	Description
Add	Add a change password rule. For more information, see Adding change password settings on page 418.
Delete	Remove the selected rule.
Refresh	Update the list of change password rules.
Edit	Modify the selected rule.
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding change password settings

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules SPP uses to reset account passwords.

> IMPORTANT: Passwords for accounts associated with a password sync group are managed based on the profile change schedule and processed via the sync group. If synchronization fails for an individual account in the sync group, the account is retried multiple times and, if failing after that, the sync task halts and is rescheduled. The administrator must correct the cause of the failure for the sync task to continue. For more information, see Password sync groups on page 427.

Navigate to **Asset Management** > **Profiles** > **View Password Profile Components** > **Change Password**.

To add a password reset schedule

1. Click **+Add** to open the **Change Password Settings** dialog.
2. Enter a **Name** of up to 50 characters for the rule.
3. Enter a **Description** of up to 255 characters for the rule.
4. Select a partition using the **Browse** button.
5. Optionally, complete any of these settings:
   - **Change Passwords Manually**. For more information, see How do I manage accounts on unsupported platforms on page 663.
   - **Change the password even if release is active**: Select this option to allow a password change even when a password release is active.
   - **Require current password**: Select this option to require a current password.
   - **Suspend account when checked in**: Select this option to automatically suspend managed accounts that are not in use. That is, the account on a managed asset is suspended until a request is made for it through SPP, at which time SPP restores the account. Once the request is checked in or closed, the account is again suspended.
     Click the **supported platforms** link to display a list of platforms that support this feature.
   - **Reschedule for unscheduled password change**: Select this option to reset the password schedule when a password is manually changed. For example: a password reset is scheduled to occur every 10 days, but on day 8 the password is manually changed. Due to this manual reset, the schedule will restart so that the next password reset will occur in 10 days rather than keeping the original scheduled reset (which would have been in 2 days).

   > NOTE: All options listed below are supported only on Windows platforms. Expand the **Windows Only** section to view these options.

   - **Update service on password change (Windows Only)**: For Windows services that are configured to run as a local managed account or a dependent AD account on an asset, select this option to ensure that the password change is also applied to each service the account runs. If the service is running as a

dependent AD account, the windows asset and the dependent Active Directory account must be in the same profile.

- **Restart service on password change (Windows Only)**: For Windows services that are configured to run as a local managed account or a dependent AD account on an asset, select this option to ensure that there is an automatic restart after the password is changed. For a local account, the profile assigned to the account is used. For an AD account, the profile assigned to the asset is used.
- **Update IIS app pool on password change (Windows Only)**: For IIS App pools that are configured to run as a local managed account or a dependent AD account on an asset, select this option to ensure that the password change is also applied to each IIS App pool the account runs. If the service is running as a dependent AD account, the windows asset and the dependent Active Directory account must be in the same profile.
- **Update COM+ on password change (Windows Only)**: For Com+ applications that are configured to run as a local managed account or a dependent AD account on an asset, select this option to ensure that the password change is also applied to each COM+ application the account runs. If the service is running as a dependent AD account, the windows asset and the dependent Active Directory account must be in the same profile.
- **Update task on password change (Windows Only)**: For scheduled tasks that are configured to run as a local managed account or a dependent AD account on an asset, select this option to ensure that the password change is also applied to each task the account runs. If the service is running as a dependent AD account, the windows asset and the dependent Active Directory account must be in the same profile.

6. (Only Linux, Unix, and Windows SSH platforms) (Optional) On the **Dependent Systems** tab, click **Edit** to configure a custom dependency that will run a command on an asset to perform custom updates when a password is changed for a dependent account. The following configuration options are available:

   IMPORTANT: When configuring custom dependency commands, the following information should be kept in mind:

   - Any valid command on the asset that is accessible to the service account can be configured to run as a dependency. NO VALIDATION will be performed by Safeguard on the command.
   - You cannot discover services, or automatically configure dependencies on Linux/Unix.
   - A directory account can be manually configured as a dependent account on Linux/Unix.
   - If you add a directory account as a dependent account for a Linux/Unix asset, the asset's profile will determine the action (including any custom commands) to take when the AD account password changes.

- Local accounts are automatically dependent accounts if a custom dependency is configured in the account's password profile.
- For AD accounts, custom dependencies will only run after a successful password change; and will run on each Unix or Linux asset configured as a dependent asset, rather than on the AD asset.
- For AD accounts, any commands configured to run before a password change or after a failed password change will be ignored.

- **Run custom command before password change**: Select this option to configure a custom dependency that is run before a password change occurs on a dependent account.
  - **Command**: This is the command that will be run. It is a free format string that should identify the fully qualified path of the command to be run. It can contain tokens that will be resolved using the account details when the operation runs.

    You can use the **Insert Command Token** drop-down to add tokens to the field. For example, selecting **AssetName** will add `%{AssetName}%` to the **Command** field. The AssetName token will then be replaced when the operation is run on an asset.
  - **Command Line Arguments**: These are the arguments that will be passed on the command line. It can contain tokens that will be resolved using the account details when the operation runs. The command line arguments should be quoted appropriately (for example, an argument that contains a space must be quoted).

    You can use the **Insert Command Line Argument Token** drop-down to add tokens to the field. For example, selecting **UserKey** will add `%{UserKey}%` to the **Command Line Arguments** field.
  - **Stdin Arguments**: The is an ordered list of arguments that will be written to stdin when the command is run. Each string in the list will be written as a separate line and can contain tokens.

    You can use the **Insert Stdin Argument** button to open a dialog that allows you to enter a string value. You can also use the **Insert Stdin Argument Token** drop-down to select from a list of tokens that be included. For example, selecting **DelegationPassword** will add `%{DelegationPassword}%` as a string in the **Stdin Arguments** section.
  - **Stop On Fail**: When selected, the password change will not be run if the custom dependency command fails.
  - **Log Command**: When selected, the command to be run will be logged.
  - **Log Command Arguments**: When selected, the command line arguments will be logged.

    - **Log Stdin Arguments**: When selected, the arguments written to stdin will be logged.
    - **Log Stdout**: When selected, the output generated by the command will be logged.
- **Run custom command after successful password change**: Select this option to configure a custom dependency that is run after a successful password change on a dependent account.
    - **Command**: This is the command that will be run. It is a free format string that should identify the fully qualified path of the command to be run. It can contain tokens that will be resolved using the account details when the operation runs.

      You can use the ▼ **Insert Command Token** drop-down to add commands to the field. For example, selecting **AssetName** will add `%{AssetName}%` to the **Command** field.
    - **Command Line Arguments**: These are the arguments that will be passed on the command line. It can contain tokens that will be resolved using the account details when the operation runs. The command line arguments should be quoted appropriately (for example, an argument that contains a space must be quoted).

      You can use the ▼ **Insert Command Line Argument Token** drop-down to add commands to the field. For example, selecting **UserKey** will add `%{UserKey}%` to the **Command Line Arguments** field.
    - **Stdin Arguments**: The is an ordered list of arguments that will be written to stdin when the command is run. Each string in the list will be written as a separate line and can contain tokens.

      You can use the + **Insert Stdin Argument** button to open a dialog that allows you to enter a string value. You can also use the ▼ **Insert Stdin Argument Token** drop-down to select from a list of tokens that be included. For example, selecting **DelegationPassword** will add `%{DelegationPassword}%` as a string in the **Stdin Arguments** section.
    - **Log Command**: When selected, the command to be run will be logged.
    - **Log Command Arguments**: When selected, the command line arguments will be logged.
    - **Log Stdin Arguments**: When selected, the arguments written to stdin will be logged.
    - **Log Stdout**: When selected, the output generated by the command will be logged.
- **Run custom command after failed password change**: Select this option to configure a custom dependency that is run after a password change fails for a dependent account.

- **Command**: This is the command that will be run. It is a free format string that should identify the fully qualified path of the command to be run. It can contain tokens that will be resolved using the account details when the operation runs.

  You can use the ▼ **Insert Command Token** drop-down to add commands to the field. For example, selecting **AssetName** will add `%{AssetName}%` to the **Command** field.

- **Command Line Arguments**: These are the arguments that will be passed on the command line. It can contain tokens that will be resolved using the account details when the operation runs. The command line arguments should be quoted appropriately (for example, an argument that contains a space must be quoted).

  You can use the ▼ **Insert Command Line Argument Token** drop-down to add commands to the field. For example, selecting **UserKey** will add `%{UserKey}%` to the **Command Line Arguments** field.

- **Stdin Arguments**: The is an ordered list of arguments that will be written to stdin when the command is run. Each string in the list will be written as a separate line and can contain tokens.

  You can use the + **Insert Stdin Argument** button to open a dialog that allows you to enter a string value. You can also use the ▼ **Insert Stdin Argument Token** drop-down to select from a list of tokens that be included. For example, selecting **DelegationPassword** will add `%{DelegationPassword}%` as a string in the **Stdin Arguments** section.

- **Report of Exit Status**: When selected, the exit status will be reported to SPP and the operation will be retried. When this option is not selected, SPP will report success for the operation regardless of the result.
- **Log Command**: When selected, the command to be run will be logged.
- **Log Command Arguments**: When selected, the command line arguments will be logged.
- **Log Stdin Arguments**: When selected, the arguments written to stdin will be logged.
- **Log Stdout**: When selected, the output generated by the command will be logged.

7. On the **Schedule** tab, select **Run Every** to run the job along per the run details you enter. (If you deselect **Run Every**, the schedule details are lost.)
   - Configure the following.

     To specify the frequency without start and end times, select from the following controls. If you want to specify start and end times, go to the **Use Time Window** selection in this section.

     Enter a frequency for **Run Every**. Then, select a time frame:

- **Minutes**: The job runs per the frequency of minutes you specify. For example, **Every 30 Minutes** runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
- **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select **Runs Every 2 Hours @ 15 minutes after the hour**.
- **Days**: The job runs on the frequency of days and the time you enter.

  For example, **Every 2 Days Starting @ 11:59:00 PM** runs the job every other evening just before midnight.
- **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

  For example, **Every 2 Weeks Starting @ 5:00:00 AM** and **Repeat on these day**s with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.
- **Months**: The job runs on the frequency of months at the time and on the day you specify.

  For example, If you select **Every 2 Months Starting @ 1:00:00 AM** along with **First Saturday of the month**, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click + **Add** or − **Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter **Every 10 Minutes** and **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

  For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

  For days, enter **Every 2 Days** and set the **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.
- **(UTC) Coordinated Universal Time** is the default time zone. Select a new time zone, if desired.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

8. Click **OK**.

Account Password Rules

Account password rules govern the construction of a new password created by SPP during an automatic account password change. You can create rules governing the allowable account passwords, such as:

- Set the allowable password length in a range from 3 to 225 characters.

  IMPORTANT: The default password length for a macrocosm partition does NOT meet the password requirements for Azure AD. If you are using the Starling Connect functionality with Azure AD, you will need to set the password range between 8 and 225 characters.

- Set first characters type and last character type.
- Allow uppercase letters, lowercase letters, numbers, and/or printable ASCII symbols along with the minimum amounts of each.
- Identify excluded uppercase letters, lowercase letters, numbers, and symbols.
- Identify if consecutive letters, numbers, and/or symbols can be repeated sequentially and, if allowed, set the maximum repetitions allowed.

NOTE: You select an account password rule set when defining a partition's profile. For more information, see Creating a password profile on page 361. An account password rule applies to all accounts governed by the profile.

Navigate to **Asset Management** > **Profiles** > **View Password Profile Components** > **Account Password Rules**.

Use these toolbar buttons to manage your account password rules.

Table 161: Account Password Rules: Toolbar

Option	Description
Add	Add an account password complexity rule. For more information, see Adding an account password rule on page 425.
Delete	Remove the selected rule.
Edit	Modify the selected rule.
Refresh	Update the list of account password rules.
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding an account password rule

It is the responsibility of the Asset Administrator, or a partition's delegated administrator, to configure account password complexity rules.

> IMPORTANT:
>
> Some Unix systems silently truncate passwords to their maximum allowed length. For example, Macintosh OS X only allows a password of 128 characters. If an Asset Administrator creates a profile with an Account Password Rule that sets the password length to 136 characters, when SPP changes the password for an account governed by that profile, the asset's operating system truncates the new password to the allowable length and does not return an error; however, the full 136-character password is stored in SPP. This causes the following issues:
>
> - Check Password for that account will fail. When SPP compares the password on the Unix host with the password in SPP, they never match because the Unix host truncated the password generated by SPP.
> - A user will not be able to log in to the Unix host account successfully with the password provided by SPP unless they truncate the password to the allowable length imposed by the operating system.

Navigate to **Asset Management** > **Profiles** > **View Password Profile Components** > **Account Password Rules**.

To add an account password rule

1. Click **+Add** to open the **New Account Password Rule** dialog.
2. Enter a **Name** for the account password rule (up to 50 characters).
3. Enter a **Description** for the account password rule (up to 255 characters).
4. Select a partition using the **Browse** button.
5. On the **Password Rules** tab, set the password requirements.
    - **Password Length**: Set a range for the password allowable length from three to 255 characters. The default is 8 to 64 characters. The maximum length must be equal to or greater than the sum of minimum characters required in the following steps. For example, if the password must have two uppercase letters, two lowercase letters, and two numeric characters, the minimum **Password Length** must be six. Note that a diacritical letter is one character.
    - **First Character Type**: Choose one of the following:
        - **All**: Alphabetical, numeric, or symbols
        - **Alphanumeric**: Alphabetical or numeric
        - **Alphabetic**: Only alphabetical characters

- **Last Character Type**: Choose one of the following:
  - **All**: Alphabetical, numeric, or symbols
  - **Alphanumeric**: Alphabetical or numeric
  - **Alphabetic**: Only alphabetical characters
- **Repeated Characters**: Choose one of the following:
  - **Allow repeated characters**: Any letters, numbers, or symbols can be repeated in any order, including consecutively.
  - **No consecutive repeated characters**: No letter, number, or symbol can be repeated after itself. You can restrict the number of consecutively repeated characters later by uppercase letters, lowercase letters, numbers, symbols, or a combination of those.
  - **No repeated characters**: All letters, numbers, or symbols can only be used once in the password.
- **Allow Uppercase**: Select to allow uppercase (capital) letters.
  - **Require a Minimum of Uppercase Characters**: Enter a number to identify the least number of uppercase letters required. To allow but not require uppercase letters, set this value at zero.
  - **Limit Consecutively Repeated Uppercase Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated uppercase letters. You must enter a **Maximum Allowed Characters** value of one or more.
  - **Exclude these Uppercase Characters**: Enter any uppercase characters you want to exclude from the password. This field is case-sensitive.
- **Allow Lowercase**: Select to allow lowercase (small) letters.
  - **Require a Minimum of Lowercase Characters**: Enter a number to identify the least number of lowercase letters required. To allow but not require lowercase letters, set this value at zero.
  - **Limit Consecutively Repeated Lowercase Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated lowercase letters. You must enter a **Maximum Allowed Characters** value of one or more.
  - **Excluded these Lowercase Characters**: Enter any lowercase characters you want to exclude from the password. This field is case sensitive.
- **Limit Consecutively Repeated Alpha Characters**: To set the number of repeated lowercase or uppercase letters combined, enter the **Maximum Allowed Characters**.

  For example, if you set the **Max Allowed** at **2** then you can not have more than two alphabet characters next to each other in the password. Using this

example, `Ab1Cd2EF` is valid but `AbC1d2EF` is not because it has three alphabet characters in a row.

- **Allow Numeric Character (0-9)**: Select to allow numeric characters in the password.
  - **Require a Minimum of Numeric Characters**: Enter a number to identify the amount of numbers required in a password. To allow but not require numbers, set this value at zero.
  - **Limit Consecutively Repeated Numeric Characters**: Select the check box to limit the number of consecutively repeated numeric characters. You must enter a **Maximum Allowed Characters** value of one or more.
  - **Exclude these Numeric Characters**: Enter any numeric characters you want to exclude from the password. This field is case sensitive.
- **Allow Symbols (e.g. @ # $ % &)**: Select this check box to allow characters that are printable ASCII characters. These often include: ~ ` ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
  - **Require a Minimum of Symbols**: Enter a number to identify the least number of symbols required. To allow but not require symbols, set this value at zero.
  - **Limit Consecutively Repeated Symbols**: If you allowed repeated characters earlier, select the check box to limit the number of symbols that can repeat consecutively. You must enter a **Maximum Allowed Characters** value of one or more.
  - Set the following:
    - **Valid Symbols**: Select this option to enter allowable special characters. Enter the allowable symbols in the **Symbol List** text box.
    - **Invalid Symbols**: Select this option to enter prohibited special characters. Enter the prohibited symbols in the **Symbol List** text box.

6. Click **Test Rule** to check the rules set.
7. When the rules are complete, click **OK**.

Password sync groups

A password sync group is used to control password validation and reset across all associated accounts. The same password is used for one or more accounts associated with the same or different assets. For example, synchronized passwords can be used for accounts that support clusters or systems that sync between development, test, and production. An account can belong to only one password sync group. Multiple password sync groups can be added to a profile.

The profile change schedule is applied to the sync group. The sync group controls the tasks to change the passwords for the accounts in the sync group. Change tasks occur in the order of password sync group account priority. If synchronization fails for an individual

account in the sync group, the account is retried multiple times and, if failing after that, the sync task halts and is rescheduled. The administrator must correct the cause of the failure for the sync task to continue.

If an account is associated with a profile with a daily check schedule and also associated with a password sync group, a mismatch on the daily check will trigger a task to set the account password to the current sync group password.

For more information, see Creating a password profile on page 361.

Password sync group account priority

When an account is added to a password sync group, the default priority is 0, which is the highest priority. Subsequent numbers are lower priority (for example, 0, 1, or 2, where 0 is the highest priority and 2 is the lowest). Priority determines the order in which account passwords are changed. If all accounts have the same priority, they are synchronized simultaneously. When different priorities are set, accounts at the highest priority (for example, 0) are synchronized first. If priority 0 is successful, accounts at the next priority are synchronized. If any account at a priority fails, the synchronization processing stops and the group is scheduled for synchronization retry. For example, a cluster of systems may have an admin account with the same password. If one primary system is set at priority 0 and the subordinates are set at priority 1, the password change on the primary must be successful before the passwords on the subordinates are changed. If the primary password change fails, the subordinates are unaffected, the cluster continues to function, password change is rescheduled, and the error is logged.

Navigate to **Asset Management** > **Profiles** > **View Password Profile Components** > **Password Sync Groups**.

Table 162: Sync Groups: Properties

Property	Description
Enable	If **Enable** is selected, the sync runs with the profile change schedule.
Status	The ✔ **Status** displays if all account passwords are in sync with the password sync group. The **Status** is ⚠ if any password for any account within the sync group does not match the common password.
Name	The name of the password sync group.
Accounts	The number of accounts to synchronize with a common password.
Next Sync Date	The date the sync group password will be synchronized across all accounts.
Description	Information about the rule.

Use the following toolbar buttons to manage password sync groups.

NOTE: Changes made from the **Password Sync Groups** pane are reflected in the password sync groups in the profile. See Creating a password profile.

Table 163: Sync Groups: Toolbar

Option	Description
Add	Add a password sync group. For more information, see Adding a password sync group on page 429.
Delete	Permanently remove the selected password sync group.
View Details	Modify the selected password sync group rule.
Change Sync Group Password	Change the password for the selected sync group. All accounts in the password sync group synchronize with the new password.
Refresh	Update the list of password sync groups.
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding a password sync group

The Asset Administrator or a partition's delegated administrator defines the password sync group. An account can belong to only one password sync group. To assign sync groups and related accounts when adding the profile to a partition, see Creating a password profile.

To create a password sync group

1. On the **New Password Sync Group** dialog, enter a unique **Name** of up to 100 characters.
2. Enter a **Description** of up to 255 characters.
3. Once the Password Sync group has been saved, click **Edit**.
4. Open the Accounts tab.
5. Click **Add** and select one or more **Accounts** to be synchronized.
6. The **Accounts** list displays with information about the account. Click any of the columns to sort the accounts.
7. Click **Select Accounts**. The following values display:
   - **Status**: Displayed as if the password is not the same as the sync group, if the password is the same, or if the account is ignored and possibly should not be in the sync group.

- **Priority**: The default is priority 0 (the highest). To change the priority, double-click the **Priority** value and enter the new priority. For more information, see Password sync group account priority on page 428.
- **System Name**: Name of the system (asset) assigned that is associated with the account.
- **Account Name**: Name of the account.
- **Domain Name**: Name of the domain.
- **Last Sync Time**: The date and time of the last sync.

8. Click **OK**.

Setting a default password profile

When you create a new partition, SPP creates a corresponding default profile with default schedules and rules.

To set another password profile as the default

1. Navigate to **Asset Management** > **Profiles**.
2. In Password Profiles, select a profile that is not the current default profile for a partition.
3. Click **Set as Default** from the details toolbar.

Deleting a password profile

It is the responsibility of the Asset Administrator to manage password profiles.

To delete a password profile

1. Navigate to **Asset Management** > **Profiles** > **Password Profiles**.
2. Select the profile to be deleted.
3. Click **Delete**.
4. Confirm your request.

SSH Key Profiles (profiles)

Within the web client, the **SSH Key Profiles** tab on the **Profiles** page displays information on the currently configured SSH key profiles in use by SPP.

To access the **SSH Key Profiles** tab on the **Profiles** page:

- web client: Navigate to **Asset Management** > **Profiles** and open the **SSH Key Profiles** tab. If needed, you can use the partition drop-down to select the parent partition of the profile (by default all profiles are displayed). Select a profile, then click to display additional information and options.

Selecting one of the profiles displays the following information:

- **General** tab: Displays the name and information about this profile.
- **Check SSH Key** tab: These are the rules SPP uses to verify account SSH keys. For more information, see Adding SSH key check settings on page 436.
- **Change SSH Key** tab: These are the rules used to reset account SSH keys. For more information, see Adding SSH key change settings on page 439.
- **Discover SSH Key** tab: These are the rules used to discover SSH keys. For more information, see Adding SSH key discovery on page 445.
- **SSH Key Sync Groups** tab: You can use the **SSH Key Sync Groups** tab to add or update an SSH key sync group governed by the profile change schedule. For more information, see SSH Key Sync Groups settings on page 446.

Toolbar

Use these toolbar buttons to manage profiles:

- **New Profile**: Add profiles to SPP.
- **Delete**: Remove the selected profile.
- **View Details**: Select a profile then click this button to open additional information and options for the profile.
- **Set as Default**: Select a profile then click this button to set it as the default profile.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of profiles.

When the **SSH Key Profiles** tab on the **Profiles** page is selected, a **View SSH Key Profile Components** link is available. For more information, see View SSH Key Profile Components (profiles).

View SSH Key Profile Components (profiles)

When the **SSH Key Profiles** tab on the **Profiles** page is selected, a **View SSH Key Profile Components** link is available. This link displays information on the currently configured SSH Key profile components in use by SPP.

To open the **View SSH Key Profile Components** link on the **Profiles** page:

- web client: Navigate to **Asset Management** > **Profiles** > **SSH Key Profiles** and click the **View SSH Key Profile Components** link.

The **View SSH Key Profile Components** view contains the following tabs:

- **Check SSH Key**: This tab provides information on the currently configured check SSH key schedules. You can use the **Refresh** button to update the listed schedules.
- **Change SSH Key**: This tab provides information on the currently configured change SSH key schedules. You can use the **Refresh** button to update the listed schedules.
- **Discover SSH Key**: This tab provides information on the currently discovered SSH keys. You can use the **Refresh** button to update the listed keys.
- **SSH Key Sync Groups**: This tab provides information on the currently configured SSH key sync groups. From this tab the following options are available:
  - **Delete**: Remove the selected SSH key sync group.
  - **View Details**: View details for the selected SSH key sync group.
  - **Enable-Disable**: Use these buttons to either enable or disable the SSH key sync group.
  - **Change Sync Group Password**:
  - **Refresh**: Update the listed SSH key sync groups.

Managing SSH key profiles

Use the controls and tabbed pages on the **Profiles** page to perform the following tasks to manage SSH key profiles:

- Adding an SSH key profile
- SSH Key Profiles
- Setting a default SSH key profile
- Deleting an SSH key profile

Adding an SSH key profile

It is the responsibility of the Asset Administrator to add SSH key profiles to SPP.

To add an SSH key profile

1. Navigate to **Asset Management** > **Profiles** > **SSH Key Profiles**.
2. Click **+ New Profile** from the toolbar.
3. In the **New SSH Key Profile**dialog, enter the following information:
   a. **Name**: Enter a unique name for the partition. Limit: 50 characters.
   b. **Description**: (Optional) Enter information about this partition. Limit: 255 characters.
4. Select a partition for the SSH key profile using the **Browse** button.
5. On the **Check SSH Key** tab, select a previously defined check SSH Key setting from the drop-down menu or click **+ Add** to add a new check SSH Key setting. For more information, see Check SSH Key settings.
6. On the **Change SSH Key** tab, select a previously defined change SSH Key setting from the drop-down menu or click **+ Add** to add a new change SSH Key setting. For more information, see Change SSH Key settings.
7. On the **Discover SSH Key** tab, select a previously defined discover SSH Key setting from the drop-down menu or click **+ Add** to add a new discover SSH Key setting. For more information, see Discover SSH Key settings.
8. Click **OK** to save the SSH key profile.

   Once saved you can edit the profile to add SSH key sync groups to your SSH key profile. For more information, see SSH Key Sync Groups settings.

SSH Key Profiles

SSH authorization keys are managed to maximize security over automated processes as well as sign-on by system administrators, power users, and others who use SSH keys for access. Safeguard for Privileged Passwords (SPP) performs the following.

NOTE: SPP does not currently manage the options for an authorized key. If an imported key has any options configured in the authorized keys file on the asset, these options will not be preserved when the key is rotated by SPP.

- SPP provisions keys by creating a new key pair associated with a managed account. Any of the following methods can be used.
  - An authorized key is added in the target account on the target host. A managed account can have more than one authorized key, however only one key can be managed by SPP at a time.
  - An SSH key sync group is created for an SSH key pair. The new key is generated for the sync group and configured for each of the synced accounts on the target host. All accounts in the SSH key sync group synchronize the SSH Key so the same key can be used to log into all systems.

    - A legacy SSH identity key is uploaded. The legacy SSH key is entrusted to SPP. When legacy SSH keys are exposed, SPP rotates them after they are checked in. SPP may rotate the keys after they are checked in if the **Entitlement Policy** > **Access Configuration** option specifies **Change SSH Key after check-in**.
- SPP requests and rotates SSH keys based on the access request policy (key and session) as well as via A2A when A2A is configured to request and retrieve SSH keys. Rotation is profile-based. Each managed account can have a single SSH key.

Supported implementations

SSH implementations supported include:

- Access requests provide SSH identity keys include **OpenSSH**, **SSH2**, and **PuTTY** format.
- For management, SPP supports OpenSSH file formats and Tectia

Supported key types and key lengths

SPP supports RSA, Ed25519, ECDSA, and DSA algorithms for SSH identity keys. Supported key lengths follow:

- RSA: 1024, 2048, 4096, and 8192-bit
  Larger key sizes take longer to generate. In particular, a key size of 8192-bits may take several minutes.
- DSA: fixed to 1024-bits
- Ed25519: fixed to 32 bits
- ECDSA: 256, 384, and 521 bits

Unsupported algorithms and key strings

SPP reads each line when parsing an `authorized_keys` file and attempts to extract the data. If a line is properly formatted according to the specification, SPP will report it as a discovered identity key. SPP recognizes keys with either the RSA or DSA algorithm. Other valid key types are still discovered by SPP and are identified as the **Key Type** of **Unknown** on the Discovered SSH Keys properties grid.

Management

It is the responsibility of the Appliance Administrator to manage the access request and SSH key passphrase management services.

SSH key change, check, and discovery can be toggled on or off. For more information, see Global Services.

Navigate to **Asset Management** > **Profiles** > **SSH Key Profiles**.

Table 164: SSH Key Management settings

Setting	Description
Change SSH Key settings	You can add, update, schedule, or remove SSH Key Change settings.
Check SSH Key settings	You can add, update, schedule, or remove SSH Key Check settings.
Discover SSH Key settings	You can add, update, schedule, or remove SSH Key Discovery jobs.
SSH Key Sync Groups settings	You can add, update, schedule, or remove SSH Key Sync Group settings. The Asset Administrator or a partition's delegated administrator defines the SSH key sync group for an SSH key pair. The new key is generated for the sync group and configured for each of the synced accounts on the target host. All accounts in the SSH key sync group synchronize so the same key can be used to log into all systems.

Check SSH Key settings

Safeguard for Privileged Passwords requests and rotates SSH keys based on the access request policy (SSH key or SSH session requests) as well as via A2A configurations set up to request and retrieve SSH keys. Rotation is profile-based. Each managed account can have a single managed SSH key.

SSH key check can be toggled on or off. For more information, see Global Services.

Navigate to **Asset Management** > **Profiles** > **View SSH Key Profiles** > **Check SSH Key**.

Table 165: Check SSH Key properties

Setting	Description
Name	The name of the SSH key
Partition	The partition where the SSH key is managed
Description	Information about the SSH key
Schedule	Designates when the SSH key is checked

Use the following toolbar buttons to manage checking the SSH key.

Table 166: Check SSH Key: Toolbar

Option	Description
Add	Add SSH key check settings.
Delete	Permanently remove the selected SSH key.
Edit	Modify the selected SSH key.
Refresh	Update the list of SSH keys.
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding SSH key check settings

It is the responsibility of the Asset Administrator or the partition's delegated administrator to define the rules SPP uses to verify SSH keys.

Navigate to **Asset Management** > **Profiles** > **View SSH Key Profiles** > **Check SSH Key**.

To add an SSH key validation schedule

1. Click **Add** to open the **Check SSH Key Settings** dialog.
2. Enter a **Name** of up to 50 characters for the rule.
3. Enter a **Description** of up to 255 characters for the rule.
4. **Browse** to select a partition.
5. Optionally, complete either of these settings:
   - **Reset SSH Key on Mismatch**: Select this option to automatically reset an SSH key passphrase when SPP detects the SSH key passphrase in the appliance database differs from the SSH key passphrase on the asset.
   - **Notify Delegated Owners on Mismatch**: Select this option to trigger a notification when SPP detects an SSH key passphrase mismatch.

     NOTE: To send event notifications to a user, you must configure SPP to send alerts. For more information, see Configuring alerts on page 95. Set up an email template for the Check Mismatch event type for passwords and SSH key passphrases.
6. To change the **Check SSH Key** schedule, open the **Schedule** tab. The default is **Never**.
7. In the **Schedule** dialog, select **Run Every** to run the job along per the run details you enter. (If you deselect **Run Every**, the schedule details are lost.)

- Configure the following.

  To specify the frequency without start and end times, select from the following controls. If you want to specify start and end times, go to the **Use Time Window** selection in this section.

  Enter a frequency for **Run Every**. Then, select a time frame:

  - **Minutes**: The job runs per the frequency of minutes you specify. For example, **Every 30 Minutes** runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
  - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select **Runs Every 2 Hours @ 15 minutes after the hour**.
  - **Days**: The job runs on the frequency of days and the time you enter.

    For example, **Every 2 Days Starting @ 11:59:00 PM** runs the job every other evening just before midnight.
  - **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

    For example, **Every 2 Weeks Starting @ 5:00:00 AM** and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.
  - **Months**: The job runs on the frequency of months at the time and on the day you specify.

    For example, If you select **Every 2 Months Starting @ 1:00:00 AM** along with **First Saturday of the month**, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click + **Add** or − **Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter **Every 10 Minutes** and **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

For days, enter **Every 2 Days** and set the **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

- **(UTC) Coordinated Universal Time** is the default time zone. Select a new time zone, if desired.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

8. Click **OK**.

Change SSH Key settings

Safeguard for Privileged Passwords requests and rotates SSH keys based on the access request policy (SSH key or SSH session requests) as well as via A2A configurations set up to request and retrieve SSH keys. Rotation is profile-based. Each managed account can have a single managed SSH key.

SSH key change can be toggled on or off. For more information, see Global Services.

Navigate to **Asset Management** > **Profiles** > **View SSH Key Profiles** > **Change SSH Key**.

Table 167: Change SSH Key properties

Setting	Description
Name	The name of the SSH key
Partition	The partition where the SSH key is managed
Description	Information about the SSH key
Schedule	Designates when the SSH key is changed

Use the following toolbar buttons to manage changing the SSH key.

Table 168: Change SSH Key: Toolbar

Option	Description
Add	Add SSH key change settings. For more information, see Adding SSH key change settings on page 439.
Delete	Permanently remove the selected SSH key.
Edit	Modify the selected SSH key.
Refresh	Update the list of SSH keys.

Option	Description
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding SSH key change settings

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules SPP uses to reset SSH key passphrases.

IMPORTANT: Passphrases for accounts associated with an SSH key sync group are managed based on the profile change schedule and processed via the SSH key sync group. If synchronization fails for an individual account in the sync group, the account is retried multiple times and, if failing after that, the sync task halts and is rescheduled. The administrator must correct the cause of the failure for the sync task to continue. For more information, see SSH Key Sync Groups settings on page 446.

To add an SSH key reset schedule

1. Navigate to **Asset Management** > **Profiles** > **View SSH Key Profile Components** > **Change SSH Key**.
2. Click **+ Add** to open the **Change SSH Key Settings** dialog.
3. Enter a **Name** of up to 50 characters for the rule.
4. Enter a **Description** of up to 255 characters for the rule.
5. **Browse** to select a partition.
6. Enter a **Comment**.
7. Select a **Key Length** such as 1024, 2048, 4096, or 8192 characters. Larger key sizes take longer to generate. In particular, a key size of 8192-bits may take several minutes.
8. (Optional) Select **Change SSH Keys Manually**.

   For more information, see How do I manage accounts on unsupported platforms on page 663.
9. (Optional) **Suspend account when checked in**: Select this option to automatically suspend managed accounts that are not in use. That is, the account on a managed asset is suspended until a request is made for it through SPP, at which time SPP restores the account. Once the request is checked in or closed, the account is again suspended.
10. (Optional) **Reschedule for unscheduled SSH key change**: Select this option to reset the change SSH key schedule when it has been manually changed. For example: an SSH key change is scheduled to occur every 10 days, but on day 8 the SSH key is manually changed. Due to this manual reset, the schedule will restart so that the next SSH key change will occur in 10 days rather than keeping the original scheduled change (which would have been in 2 days).
11. To change the **Change SSH Key** schedule, open **Schedule** tab. The default is **Never**.

12. (Only Linux, Unix, and Windows SSH platforms) (Optional) On the **Dependent Systems** tab, click **Edit** to configure a custom dependency that will run a command on the dependent asset before changing the SSH key. The following configuration options are available:

> IMPORTANT: When configuring custom dependency commands, the following information should be kept in mind:
>
> - Any command on the asset that is accessible to the service account can be configured to run as a dependency. NO VALIDATION will be performed by Safeguard on the command.
> - Only applies to local accounts. SSH key changes are not available for AD accounts.

- **Run custom command before SSH Key change**: Select this option to configure a custom dependency that is run before an SSH key change occurs on a dependent account.
  - **Command**: This is the command that will be run. It is a free format string that should identify the fully qualified path of the command to be run. It can contain tokens that will be resolved using the account details when the operation runs.

    You can use the **Insert Command Token** drop-down to add commands to the field. For example, selecting **AssetName** will add `%{AssetName}%` to the **Command** field.
  - **Command Line Arguments**: These are the arguments that will be passed on the command line. It can contain tokens that will be resolved using the account details when the operation runs. The command line arguments should be quoted appropriately (for example, an argument that contains a space must be quoted).

    You can use the **Insert Command Line Argument Token** drop-down to add commands to the field. For example, selecting **UserKey** will add `%{UserKey}%` to the **Command Line Arguments** field.
  - **Stdin Arguments**: The is an ordered list of arguments that will be written to stdin when the command is run. Each string in the list will be written as a separate line and can contain tokens.

    You can use the **Insert Stdin Argument** button to open a dialog that allows you to enter a string value. You can also use the **Insert Stdin Argument Token** drop-down to select from a list of tokens that be included. For example, selecting **DelegationPassword** will add `%{DelegationPassword}%` as a string in the **Stdin Arguments** section.
  - **Stop On Fail**: When selected, the SSH key change will not be run if the custom dependency command fails.
  - **Log Command**: When selected, the command to be run will be logged.

- **Log Command Arguments**: When selected, the command line arguments will be logged.
- **Log Stdin Arguments**: When selected, the arguments written to stdin will be logged.
- **Log Stdout**: When selected, the output generated by the command will be logged.

- **Run custom command after successful SSH Key change**: Select this option to configure a custom dependency that is run after a successful SSH key change on a dependent account.
  - **Command**: This is the command that will be run. It is a free format string that should identify the fully qualified path of the command to be run. It can contain tokens that will be resolved using the account details when the operation runs.

    You can use the ▼ **Insert Command Token** drop-down to add commands to the field. For example, selecting **AssetName** will add `%{AssetName}%` to the **Command** field.
  - **Command Line Arguments**: These are the arguments that will be passed on the command line. It can contain tokens that will be resolved using the account details when the operation runs. The command line arguments should be quoted appropriately (for example, an argument that contains a space must be quoted).

    You can use the ▼ **Insert Command Line Argument Token** drop-down to add commands to the field. For example, selecting **UserKey** will add `%{UserKey}%` to the **Command Line Arguments** field.
  - **Stdin Arguments**: The is an ordered list of arguments that will be written to stdin when the command is run. Each string in the list will be written as a separate line and can contain tokens.

    You can use the + **Insert Stdin Argument** button to open a dialog that allows you to enter a string value. You can also use the ▼ **Insert Stdin Argument Token** drop-down to select from a list of tokens that be included. For example, selecting **DelegationPassword** will add `%{DelegationPassword}%` as a string in the **Stdin Arguments** section.
  - **Log Command**: When selected, the command to be run will be logged.
  - **Log Command Arguments**: When selected, the command line arguments will be logged.
  - **Log Stdin Arguments**: When selected, the arguments written to stdin will be logged.
  - **Log Stdout**: When selected, the output generated by the command will be logged.

- **Run custom command after failed SSH Key change**: Select this option to configure a custom dependency that is run after an SSH key change fails for a dependent account.
  - **Command**: This is the command that will be run. It is a free format string that should identify the fully qualified path of the command to be run. It can contain tokens that will be resolved using the account details when the operation runs.

    You can use the **Insert Command Token** drop-down to add commands to the field. For example, selecting **AssetName** will add `%{AssetName}%` to the **Command** field.
  - **Command Line Arguments**: These are the arguments that will be passed on the command line. It can contain tokens that will be resolved using the account details when the operation runs. The command line arguments should be quoted appropriately (for example, an argument that contains a space must be quoted).

    You can use the **Insert Command Line Argument Token** drop-down to add commands to the field. For example, selecting **UserKey** will add `%{UserKey}%` to the **Command Line Arguments** field.
  - **Stdin Arguments**: The is an ordered list of arguments that will be written to stdin when the command is run. Each string in the list will be written as a separate line and can contain tokens.

    You can use the **Insert Stdin Argument** button to open a dialog that allows you to enter a string value. You can also use the **Insert Stdin Argument Token** drop-down to select from a list of tokens that be included. For example, selecting **DelegationPassword** will add `%{DelegationPassword}%` as a string in the **Stdin Arguments** section.
  - **Report of Exit Status**: When selected, the exit status will be reported to SPP and the operation will be retried. When this option is not selected, SPP will report success for the operation regardless of the result.
  - **Log Command**: When selected, the command to be run will be logged.
  - **Log Command Arguments**: When selected, the command line arguments will be logged.
  - **Log Stdin Arguments**: When selected, the arguments written to stdin will be logged.
  - **Log Stdout**: When selected, the output generated by the command will be logged.

13. In the **Schedule** dialog, select **Run Every** to run the job along per the run details you enter. (If you deselect **Run Every**, the schedule details are lost.)

- Configure the following.

  To specify the frequency without start and end times, select from the following controls. If you want to specify start and end times, go to the **Use Time Window** selection in this section.

  Enter a frequency for **Run Every**. Then, select a time frame:

  - **Minutes**: The job runs per the frequency of minutes you specify. For example, **Every 30 Minutes** runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
  - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select **Runs Every 2 Hours @ 15 minutes after the hour**.
  - **Days**: The job runs on the frequency of days and the time you enter.

    For example, **Every 2 Days Starting @ 11:59:00 PM** runs the job every other evening just before midnight.
  - **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

    For example, **Every 2 Weeks Starting @ 5:00:00 AM** and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.
  - **Months**: The job runs on the frequency of months at the time and on the day you specify.

    For example, If you select **Every 2 Months Starting @ 1:00:00 AM** along with **First Saturday of the month**, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click + **Add** or − **Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter **Every 10 Minutes** and **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

For days, enter **Every 2 Days** and set the **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

- **(UTC) Coordinated Universal Time** is the default time zone. Select a new time zone, if desired.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

14. Click **OK**.

Discover SSH Key settings

If an SSH key is discovered for an account on an asset, it is by definition an authorized key. An authorized key is a public SSH key that has been added to the relevant file in a user's home directory on an asset so the user can employ the corresponding private key to log in.

SSH Key Discovery jobs are run to discover and manage SSH keys. For more information, see SSH Key Discovery on page 398.

Navigate to **Asset Management** > **Profiles** > **View SSH Key Profiles** > **Discover SSH Key**.

Table 169: Discover SSH Key properties

Setting	Description
Name	The name of the SSH Key Discovery job
Partition	The partition in which to manage the discovered SSH key
Description	Information about the rule
Schedule	Designates when the SSH Key Discovery job runs

Use the following toolbar buttons to manage the SSH Key Discovery job.

Table 170: Discover SSH Key: Toolbar

Option	Description
Add	Add an SSH Key Discovery job. For more information, see Adding SSH key discovery on page 445.
Delete	Permanently remove the selected SSH Key Discovery job.
Edit	Modify the selected SSH Key Discovery job.
Refresh	Update the list of SSH Key Discovery jobs.

Option	Description
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding SSH key discovery

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules that govern how SPP performs SSH key discovery. For more information, see Account Discovery job workflow on page 384.

To add an SSH Key Discovery job

1. Navigate to **Asset Management** > **Profiles** > **View SSH Key Profiles** > **Discover SSH Key**.
2. Click **+ Add** to open the **Discover SSH Key Settings** dialog.
3. Provide the following:
   a. **Name**: Enter a name for the SSH Key Discovery job. Limit: 50 characters.
   b. **Description**: Enter descriptive text about the SSH Key Discovery job. Limit: 255 characters.
   c. **Partition**: **Browse** to select a partition.
   d. To change the **Discover SSH Key** schedule, open the **Schedule** tab. The default is **Never**.
   e. On the **Schedule** tab, choose an interval for to run the SSH Key Discovery job.

      Select **Run Every** to run the job along per the run details you enter. (If you deselect **Run Every**, the schedule details are lost.)

      - Configure the following.

        To specify the frequency without start and end times, select from the following controls. If you want to specify start and end times, go to the **Use Time Window** selection in this section.

        Enter a frequency for **Run Every**. Then, select a time frame:

        - **Minutes**: The job runs per the frequency of minutes you specify. For example, **Every 30 Minutes** runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
        - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select **Runs Every 2 Hours @ 15 minutes after the hour**.
        - **Days**: The job runs on the frequency of days and the time you enter.

For example, **Every 2 Days Starting @ 11:59:00 PM** runs the job every other evening just before midnight.

- **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

  For example, **Every 2 Weeks Starting @ 5:00:00 AM** and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.

- **Months**: The job runs on the frequency of months at the time and on the day you specify.

  For example, If you select **Every 2 Months Starting @ 1:00:00 AM** along with **First Saturday of the month**, the job will run at 1 a.m. on the first Saturday of every other month.

- Select **Use Time Windows** if you want to enter the **Start** and **End** time. You can click + **Add** or — **Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

  For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

  Enter **Every 10 Minutes** and **Use Time Windows**:

  - **Start 10:00:00 PM** and **End 11:59:00 PM**
  - **Start 12:00:00 AM** and **End 2:00:00 AM**

    An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

  If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

  For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

  For days, enter **Every 2 Days** and set the **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

- **(UTC) Coordinated Universal Time** is the default time zone. Select a new time zone, if desired.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

4. Click **OK**.

SSH Key Sync Groups settings

The Asset Administrator or a partition's delegated administrator defines the SSH key sync group for an SSH key pair. The new key is generated for the sync group and configured for

each of the synced accounts on the target host. All accounts in the SSH key sync group synchronize so the same key can be used to log into all systems.

An SSH key sync group is used to control validation and reset across all associated accounts. The same SSH key is used for one or more accounts associated with the same or different assets. For example, synchronized SSH keys can be used for accounts that support clusters or systems that sync between development, test, and production.

An account can belong to only one SSH key sync group. Multiple SSH key sync groups can be added to a profile.

The profile change schedule is applied to the SSH key sync group. The SSH key sync group controls the tasks to change the SSH keys for the accounts in the sync group. If synchronization fails for an individual account in the SSH key sync group, the account is retried multiple times and, if failing after that, the sync task halts and is rescheduled. The administrator must correct the cause of the failure for the sync task to continue.

If an account is associated with a profile with a daily check schedule and also associated with an SSH key sync group, a mismatch on the daily check will trigger a task to set the SSH key to the current SSH key.

Navigate to **Asset Management** > **Profiles** > **View SSH Key Profile Components** > **SSH Key Sync Groups**.

Table 171: SSH Key Sync Groups properties

Setting	Description
Enabled	If **Enable** is selected, the sync runs with the profile change schedule. Use the following toolbar buttons to enable or disable: • **Enable** • **Disable**
Status	The **Status** displays if all SSH key pairs are in sync with the SSH key sync group. The **Status** is if any SSH key for any account within the sync group does not synchronize.
Name	The name of the SSH key sync group
Partition	The partition that uses the rule
Profile	The profile that uses the rule
Accounts	The number of accounts to synchronize with the SSH key sync group
Next Sync Date	The date the SSH key sync group's SSH key pair will be synchronized across all accounts
Description	Information about the rule

Use the following toolbar buttons to manage SSH key sync groups.

NOTE: Changes made from the **SSH Key Sync Groups** pane are reflected in the SSH key sync groups in the profile. See Creating a password profile.

Table 172: SSH Key Sync Groups: Toolbar

Option	Description
Add	Add an SSH key sync group. For more information, see Adding SSH key sync groups on page 448.
Delete	Permanently remove the selected SSH key sync group.
View Details	Modify the selected SSH key sync group rule.
Change Sync Group SSH Keys	Change the SSH key for the selected SSH key sync group. All accounts in the SSH key sync group synchronize with the new SSH key.
Refresh	Update the list of SSH key sync groups.
Search	To locate a value in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Adding SSH key sync groups

The Asset Administrator or a partition's delegated administrator defines an SSH key sync group. An account can belong to only one SSH key sync group. To assign SSH key sync groups and related accounts when adding the profile to a partition, see Creating a password profile.

To add an SSH key sync group

1. Navigate to **Asset Management** > **Profiles** > **View SSH Key Profile Components** > **SSH Key Sync Groups**.
2. Click **Add** to open the **New SSH Key Sync Group** dialog.
3. Enter a unique **Name** of up to 100 characters.
4. Enter a **Description** of up to 255 characters.
5. Click **Browse** to select an SSH Key Profile.

   NOTE: Multiple SSH sync groups can be added to a profile. The profile change schedule is applied to the sync group. The sync group controls the tasks to change the SSH identity keys for the accounts in the sync group.
6. Click **Select SSH Key Profile**.
7. Click **OK** to save the group.
8. Once saved, select the newly added SSH Key sync group from the list and click **View Details**.
9. Open the **Accounts** tab.

10. Click **Edit**.
11. Click **+ Add** and select one or more **Accounts** to be synchronized.
12. Click **Select Accounts**.
13. Click **OK**.

Setting a default SSH key profile

When you create a new partition, SPP creates a corresponding default profile with default schedules and rules.

To set another SSH key profile as the default

1. Navigate to **Asset Management** > **Profiles**.
2. In SSH Key Profiles, select a profile that is not the current default profile for a partition.
3. Click **Set as Default** from the details toolbar.

Deleting an SSH key profile

It is the responsibility of the Asset Administrator to manage SSH key profiles.

To delete an SSH key profile

1. Navigate to **Asset Management** > **Profiles** > **SSH Key Profiles**.
2. Select the profile to be deleted.
3. Click **Delete**.
4. Confirm your request.

Tags

On the web client, Asset Administrators can create and manage tags.

- web client: Use **Asset Management** > **Tags** to create and manage tags for assets and asset accounts.

In addition, Asset Administrators can manually add static tags to assets and accounts on the **General** tab of the **Assets** or **Accounts** view. For more information, see Manually adding a tag to an asset and Manually adding a tag to an account.

The **Tags** page provides a centralized view of all the tags defined for assets and asset accounts, regardless of how they were assigned. It displays the following details.

Table 173: Tags: Properties

Property	Description
Name	The name assigned to the tag when it was created.
Partition	The asset partition to which the tag belongs.
Account Rules	Indicates whether there is a rule associated with the selected tag. A check mark in this column indicates that the tag has an account rule.
Asset Rules	Indicates whether there is a rule associated with the selected tag. A check mark in this column indicates that the tag has an asset rule.
Description	Information about the tag.
Assigned Owners	Information on the owner(s).

Use these toolbar buttons to manage tags.

Table 174: Tags: Toolbar

Option	Description
New Tag	Add a tag. For more information, see Adding a tag for tagging of assets or asset accounts on page 451.
Delete	Remove the selected tag. For more information, see Deleting an asset or asset account tag on page 456.
View Details	View details for the selected tag. For more information, see Modifying an asset or asset account tag on page 457. NOTE: You cannot modify the partition assignment of an existing tag using the **Edit** operation. Use the **Copy** operation to clone the tag and assign it to an additional partition. Use the **Delete** operation to remove the tag from the existing partition.
Copy	Clone the selected tag and assign it to one or more additional partitions. For more information, see Copying an asset or asset account tag to another partition on page 457. NOTE: If the tag already exists in the partition, the tag will be replaced with the cloned one.
Occurrences	View a list of assets and asset accounts that are assigned to the selected tag. For more information, see Viewing asset and asset account tag assignments on page 457.
Refresh	Update the list of tags.
Search	Search for a specific tag or set of tags in this list.

Adding a tag for tagging of assets or asset accounts

Use the **+New Tag** button on the **Tags** page to add a tag for an asset or asset account.

To add an asset or asset account tag

1. Navigate to **Asset Management** > **Tags**.
2. Click the **+New Tag** toolbar button.
3. On the **General** tab, enter the following information:
   - **Name**: Enter a unique name for the tag.
   - **Description**: Enter information about the tag.
   - **Partition**: Click **Browse** to select the partition to which this tag is to be assigned.
4. On the **Asset Rules** tab, enter the conditions for an asset rule.
   - **Enable rule for this tag**: Select this check box to enable the configured rule for the tag.
   - **Rule editor**: Use the rule editor to define conditions for tagging assets.

Table 175: Asset Rules tab: Rule editor controls

Property	Description
AND | **OR**	Click **AND** to group multiple search criteria together, where all criteria must be met in order to be included. Click **OR** to group multiple search criteria together, where at least one of the criteria must be met in order to be included.
Attribute	In the first query clause box, select the attribute to be searched. Valid attributes include: • **Allow Session Requests** • **Description** • **Directory Container** (If you use the operator **Equal**, one level is found.) • **Disabled** • **Discovered Group Distinguished Name** (Use this selection to specify the search is for the domain to which the group belongs.) • **Discovered Group Name** (Use this selection to

Property	Description

	not specify the domain in the search. To specify the domain, select **Discovered Group Distinguished Name**.)
	• **Discovery Job Name**
	• A profile selection: Profiles can be inherited. For example, an account can be assigned to a specific profile (**Profile Name**) or it can inherit the profile from its parent asset (**Effective Profile Name**). When inherited, **Profile Name** will be null. **Effective Profile Name** will always have a value.
	  • **Effective Profile Name**
	  • **Profile Name**
	• **Name** (default)
	• **Network Address**
	• **Partition Name**
	• **Platform**
	• **Tag**

Operator	In the middle clause query box, select the operator to be used in the search. The operators available depend on the data type of the attribute selected. For string attributes, the operators may include: • Contains (Default) • Does Not Contain • Starts With • Ends With • Equals • Matches • Does Not Equal For boolean attributes, the operators may include: • Is True • Is False
Enter condition value	In the last clause query box, enter the search string or value to be used to find a match.
+ | −	Click + to the left of a search clause to add an additional

Property	Description
	clause to the search criteria. Click **−** to remove the search clause from the search criteria.
Add Grouping | **Remove**	Click the **Add Grouping** button to add an additional set of conditions to be met. A new grouping is added under the last query clause in a group and appears in a bordered pane showing that it is subordinate to the higher level query conditions. Click the **Remove** button to remove a grouping from the search criteria.
Preview	Click **Preview** to run the query in order to review the results of the query before adding the dynamic tag.

5. On the **Account Rules** tab, enter the conditions for an account rule.
   - **Enable rule for this tag**: Select this check box if you want to include an account rule.
   - **Rule editor:** Use the rule editor to define conditions for tagging asset accounts.

Table 176: Asset Account Rules tab: Rule editor controls

Property	Description
AND | **OR**	Click **AND** to group multiple search criteria together, where all criteria must be met in order to be included. Click **OR** to group multiple search criteria together; where at least one of the criteria must be met in order to be included.
Attribute	In the first query clause box, select the attribute to be searched. Valid attributes include: • **Allow Password Requests** • **Allow Session Requests** • **Allow SSH key Requests** • **Asset Name** • **Asset Tag** • **Description** • **Directory Container** (If you use the operator

Property	Description

	Equal, one level is found.)
	• **Disabled**
	• **Discovered Group Distinguished Name** (Use this selection to specify the search is for the domain to which the group belongs.)
	• **Discovered Group Name** (Use this selection to not specify the domain in the search. To specify the domain, select **Discovered Group Distinguished Name**.)
	• **Discovery Job Name**
	• **Distinguished Name**
	• **Domain Name**
	• **Name**
	• **NETBIOS Name**
	• **Partition Name**
	• Specify the platform. Here is how the search works:
	  • **Platform**: This is the broadest search which will return the most results. The value you enter matches if it is found in one or more of the following:
	  • `DisplayName` (**Platform Name**) such as Windows
	  • `PlatformType` such as MicrosoftAD, Ubuntu, RacfLdap
	  • `PlatformFamily` such as Windows, Linux, AIX
	  • `Platform.Version` (**Platform Version**) such as Server 2016, 10
	  For example, typing in `Other` could return these platforms: `Windows Other`, `Other Other`, and `Other`.
	  • **Platform Name**: For a more granular search, enter the name of the platform, such as `Windows`. If you enter `Windows` without entering a **Platform Version**, there may be a match on `Windows Server 2019`, `Windows Server 2016`, and `Windows 10`.

Property	Description
	• **Platform Version**: Enter the version of the platform, such as `Server 2016`. For a precise search, enter both the **Platform Name** and the **Platform Version**, For example, if you enter the **Platform Name** as `Windows` and the **Platform Version** as `Server 2016`, then only `Windows Server 2016` will be selected. For more information, see Supported platforms on page 33. • **Service Account** • **SID** • **Tag**
Operator	In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. For string attributes, the operators may include: • Contains (Default) • Does Not Contain • Starts With • Ends With • Equals • Does Not Equal • Matches For boolean attributes, the operators may include: • Is True • Is False
Enter condition value	In the last clause query box, enter the search string or value to be used to find a match.
+ | −	Click + to the left of a search clause to add an additional clause to the search criteria. Click − to remove the search clause from the search criteria.
Add Grouping | Remove	Click the +**Add Grouping** button to add an additional set of conditions to be met. A new grouping is added under the last query clause in a

Property	Description
	group and appears in a bordered pane showing that it is subordinate to the higher level query conditions. Click the **Remove** button to remove a grouping from the search criteria.
Preview	Click **Preview** to run the query in order to review the results of the query before adding the dynamic tag.

6. Click **OK** to create the tag, close the dialog, and return to the **Tags** pane.
7. Once the tag has been saved, select the tag and click **View Details**.
8. On the **Assigned Owners** tab, enter the users or groups associated with the tag. This does NOT mean the users and/or groups associated with the tag are the owners of the tag itself. Instead, when the tag is assigned to an asset or account, the listed users or groups will become owners of that asset or account.

Table 177: Assigned Owners tab: Rule editor controls

Property	Description
+ | −	Click + to **Add User or User Group**. Click − to remove a previously added user or group.
Refresh	Update the list of users and groups.

9. Click **OK** to save the assigned owners, close the dialog, and return to the **Tags** pane.

Deleting an asset or asset account tag

A tag can be assigned to multiple object types. That is, you can have the same tag assigned to assets and asset accounts including directory accounts. When deleted, all references to a tag will be removed, no matter how it was assigned (dynamically or manually).

To delete an asset or asset account tag

1. Navigate to **Asset Management** > **Tags**.
2. Select the tag to be deleted.
3. Click the **Delete** toolbar button.
4. On the confirmation dialog, click **Yes**.
5. If the tag is being used, removing the tag may result in changes to your policy configuration; therefore, you are given the opportunity to confirm or cancel the remove operation.
    - To remove the tag, click **Force Delete**.

Modifying an asset or asset account tag

Use the ✎ **View Details** button on the **Tags** pane on the **Asset Management** settings page to modify an asset or asset account tag.

You cannot modify the partition assignment of an existing tag using the **View Details** operation. Use the **Copy** operation to clone the tag and assign it to an additional partition. For more information, see Copying an asset or asset account tag to another partition on page 457.

To modify an asset or asset account tag

1. Navigate to **Asset Management** > **Tags**.
2. Select the tag to be modified.
3. Select the ✎ toolbar button. The **Tag** dialog displays allowing you to modify the selected tag settings. For more information, see Adding a tag for tagging of assets or asset accounts on page 451.

Copying an asset or asset account tag to another partition

Tags for assets and asset accounts belong to a partition. Use the **Copy** button on the **Tags** pane on the **Asset Management** settings page to clone an asset or asset account tag and assign it to a different partition.

You cannot modify the partition assignment of an existing tag using the **View Details** operation. Use this **Copy** operation to clone the tag and assign it to an additional partition.

To copy an asset or asset account tag to another partition

1. Navigate to **Asset Management** > **Tags**.
2. Click the toolbar button. The **Copy Tag** dialog displays, allowing you to select one or more partitions.
3. Select the check box for the partitions to which the selected tag is to be assigned.
4. Click **Select Partition**. If a tag with the same name already exits in the selected partition, you will be asked if you want to replace the tag.

Viewing asset and asset account tag assignments

Use the ⓘ **Occurrences** button on the **Tags** pane on the Asset Management page to view a list of all the assets and asset accounts assigned to a tag.

To view asset and asset account tag assignments

1. Navigate to **Asset Management** > **Tags**.
2. Select a tag from the list.
3. Click the **Occurrences** toolbar button.

   The **Occurrences** dialog displays, which contains a list of all the assets and accounts assigned to the selected dynamic tag:

   - **Name**: Name of the asset or account.
   - **Domain Name**: Name of the domain.
   - **Asset**: The name of the asset.
   - **Dynamic**: Indicates whether or not the tag is dynamically assigned.
   - **Type**: Whether the occurrence identifies an **Asset** or **Account** associated with the named **Asset**.
4. Use the Search box to locate a specific tag or set of tags in this list. Enter the character string to be used to search for a match.
5. Click ✕ to close the dialog and return to the **Tags** pane.

Registered Connectors

The Asset Administrator is responsible for adding and managing registered connectors.

Navigate to:

- web client: **Asset Management** > **Connect and Platforms** > **Registered Connectors**.

After joining SPP with One Identity Starling (for more information, see Starling), the **Registered Connectors** pane displays the following.

Table 178: Registered Connectors: Properties

Property	Description
Display	This column shows the display name entered for the registered connector.
Platform Name	This column shows the platform name.
Visible To Partitions	This column shows the partitions that the connector is visible for. When a connector is visible to all partitions then the column will show **All Partitions**.

Use the following toolbar buttons to manage the registered connector settings.

Table 179: Registered Connectors: Toolbar

Option	Description
Add	Add a registered connector. For more information, see Adding a registered connector.
Delete	Remove the selected registered connector.
Edit	Edit the selected registered connector.
Refresh	Update the list of registered connectors.
View	View the valid operations for the registered connector.

Related Topics

Adding a registered connector

Adding a registered connector

It is the responsibility of the Asset Administrator to configure registered connectors.

To add a registered connector

IMPORTANT: Before adding a registered connector, read the Starling Connect documentation for instructions on configuring the connector within Starling Connect for use with SPP. The connectors currently available for use with SPP are listed in the Starling Connect documentation.

1. Navigate to:
   - web client: **Asset Management** > **Connect and Platforms** > **Registered Connectors**.
2. Click **+ Add**.
3. These fields display:
   a. **Registered Connectors**: Select the connector (already configured in Starling Connect) to register with SPP.
   b. **Starling Connector Version**: Select the version for the Starling connector.
   c. **Display**: Enter a display name for the connector.
   d. **Visible To All Partitions**: Select this check box to make the registered connector visible to all partitions.
   e. **Visible To Partitions**: Available when **Visible To All Partitions** is not selected, use this section to define which partitions this registered connector will be visible to:

- + (**Add**): Use this button to add a new partition.
- — (**Remove**): Use this button to remove a previously selected partition.

4. To add the registered connector, click **OK**.

   The connector will now be registered as a platform and be available as a platform type in the definition of an asset.

IMPORTANT: When using a registered connector with SPP, there may be additional considerations involved when configuring certain functionalities. For example, Azure AD uses throttling to limit the number of password changes that can occur within a set period of time. This can mean errors are reported within SPP when a large number of accounts associated with a registered Azure AD connector are all scheduled to automatically update their passwords due to their password management settings.

Custom platforms

The Asset Administrator adds a custom platform that includes uploading the custom platform script with the platform's commands and details. Auditors and Partition Administrators have read only rights. Custom platforms are global across all partitions. The custom platform can be selected when adding or updating an asset.

Navigate to:

- web client: **Asset Management** > **Connect and Platforms** > **Custom Platforms**.

Use the following toolbar buttons to manage the custom platform settings.

Table 180: Custom Platforms: Toolbar

Option	Description
Add	Add a custom platform. For more information, see Adding a custom platform.
Delete	Remove the selected custom platform. **CAUTION: If the custom platform is associated with an asset, deleting the custom platform may halt password or SSH key validation and reset. A warning displays, indicating that the asset will be assigned to the Product platform type Other. Enter Force Delete to confirm the deletion.**
Edit	Edit the selected platform.
Download	Download the selected custom platform JSON script.

Option	Description
Refresh	Update the list of custom platforms.

Related Topics

Creating a custom platform script

Adding a custom platform

Creating a custom platform script

A custom platform script identifies the platform's commands and associated details. Scripts are written in JSON. Scripts include metadata, parameters, function blocks, operations, and if/then constructs to authenticate to the platform and perform password or SSH key validation and reset. The custom platform script is uploaded when adding the custom platform.

An Asset Administrator can create an asset and accept default values in the associated custom script. If you later upload a new version of the custom platform script with different defaults, the asset defaults are not changed.

A delegated administrator cannot create a custom platform script.

Sample scripts

Sample custom platform scripts and command details are available at the following links available from the on GitHub:

- Safeguard Custom Platform Home
  - The Structure of a Custom Platform Script
  - Writing A Custom Platform Script
  - Command-Reference
- Sample Scripts

CAUTION: Example scripts are provided for information only. Updates, error checking, and testing are required before using them in production. SPP checks to ensure the values match the type of the property that include a string, boolean, integer, or password (which is called secret in the API scripts). SPP cannot check the validity or system impact of values entered for custom platforms.

During development, check your JSON using a validator.

Adding a custom platform

It is the responsibility of the Asset Administrator to configure the rules so SPP handles custom platforms. The custom platform script must be available for uploading. For more information, see Creating a custom platform script on page 461.

To add a custom platform

1. Have the custom platform script file available to upload.
2. Navigate to:
   - web client: **Asset Management** > **Connect and Platforms** > **Custom Platforms**.
3. Click **+ Add**.
4. These fields display:
   a. **Name**: Enter the unique name of the platform type, which may be a product name.
   b. **Platform Script**: Click **Browse**. Navigate to and select the script file. Click **Open**. The selected custom platform script file displays.
   c. Select the **Allow Sessions Requests** check box to allow session access requests. This check box is typically selected for SSH. Clear the **Allow Sessions** check box to prohibit session access requests.
5. Click **OK**. If the custom platform script has errors, an error message like the following displays: `Definition was not a valid json object .`

Importing objects

SPP allows you to import a .csv file containing a set of accounts, assets, or users. A .csv template for import can be downloaded when you click **Import** from the toolbar then click **Download Template**. The hard limit on file size 100 MiB. For more information, see Creating an import file.

To import Assets and Users

1. Navigate to **Assets** or **Users** based on what data you are importing.
2. Click **Import** from the toolbar.
3. In the **Import** dialog, click **Import** to select an existing .csv file containing a list of objects to import.
4. Click **OK**. SPP imports the objects into its database. The dialog will update as the import progresses and will alert you should any errors be found.

To import Accounts

1. Navigate to **Accounts**.
2. Click **Import** from the toolbar.

   When importing accounts, you can import accounts, passwords and SSH keys separately. In this case, the **Import** button works as a drop-down. First, you need to import accounts. Select **Import Accounts**.

   Then, depending on what data you want to import, select **Import Passwords** or **Import SSH Keys**.
3. In the **Import** dialog, click **Import** to select an existing .csv file containing a list of objects to import.
4. Click **OK**. SPP imports the objects into its database. The dialog will update as the import progresses and will alert you should any errors be found.

When importing Starling User accounts from Microsoft Azure Active Directory (AAD), there are some expected differences.

For Starling type Identity Provider required fields are:

- **Name**: This must have an entry of the user **UserPrincipalName**. Any other entry will be overwritten.
- **PrimaryAuthenticationProvider/Name**: This will be the Starling provider name.
- **PrimaryAuthenticationProvider/Identity**: This is the AAD user Id.
- **IdentityProvider/Name**: This tells the import what type of user to import.

The following fields will be populated from the AAD user properties. An entry for these fields in the CSV import file will be overwritten by the information from AAD.

- FirstName
- LastName
- EmailAddress
- MobilePhone
- WorkPhone

For more information about asset creation, see Adding an asset.

Creating an import file

When importing objects, such as accounts, assets, or users, SPP expects the import file to be a Comma Separated Values (CSV) file.

A CSV file is a text file used to store database entries where each line is a unique record and each record consists of fields of data separated by commas. You must not add any trailing spaces in the properties you define in the CSV file. The easiest way to create a CSV file is by using a spreadsheet program such as Microsoft Excel; however, you can use any text

editor, such as Notepad, to create a comma-delineated file, as long as you save the file with a .csv file type extension.

The order of the columns is not important, but the title of the column must match the property name.

To create a customized .csv file template

1. In the **Import** dialog, click **Download Template** to save a copy of the template properties table to a location of your choice.
2. Locate the downloaded template and add your specific information to the template.
3. Use the customized .csv file to import the objects.

   For more information on columns, see Template CSV file.

Template CSV file

Clicking **Download Template** will download a template file in which the columns will match the export column names. The following is a list of columns in each template.

Asset template

The Asset template CSV contains the following columns:

- **Name**: A string containing the display name for this asset.
- **PlatformDisplayName**: A string containing the name of the Platform for this asset.
- **Description**: A string containing a description for this asset.
- **AssetPartitionName**: A string containing the name of the Partition for this asset.
- **NetworkAddress**: A string containing the network address for this asset.
- **ConnectionProperties/Port**: An integer containing the port for this asset.
- **ConnectionProperties/ServiceAccountDomainName**: A string containing the service account domain name if it has one.
- **ConnectionProperties/ServiceAccountName**: A string containing the service account name.
- **ConnectionProperties/ServiceAccountPassword**: A string containing the password to use for the service account.
- **ConnectionProperties/ServiceAccountCredentialType**: A string specifying the type of credential to use to authenticate to the asset.

  The possible values are `None`, `Password`, `SshKey`, `DirectoryPassword`, `LocalHostPassword`, `AccessKey`, `AccountPassword`, `Custom`, `Starling`.
- **ConnectionProperties/AccessKeyId**: A string containing an access key ID for AWS password management.

- **ConnectionProperties/SecretKey**: A string containing a secret key for AWS password management.
- **ConnectionProperties/ServiceAccountDistinguishedName**: A string containing the LDAP distinguished name of a service account. This is used for creating LDAP directories.
- **ConnectionProperties/UseSslEncryption**: Do not use SSL encryption for LDAP directory, valid values are true, false, or leave it empty.
- **ConnectionProperties/VerifySslCertificate**: Do not verify Server SSL certificate of LDAP directory, valid values are true, false, or leave it empty.
- **ConnectionProperties/PrivilegeElevationCommand**: A string containing the privilege elevation command, ex. sudo.
- **ConnectionProperties/ServiceAccountSshKey/PrivateKey**: A string containing the service accounts private key.
- **ConnectionProperties/ServiceAccountSshKey/Passphrase**: A string containing the passphrase to access the service account private key, blank if not needed.
- **SshHostKey/SshHostKey**: A string specifying the SSH host key for this asset.

AssetAccount template

The AssetAccount template CSV contains the following columns:

- **Name**: A string containing the name for the account.
- **Description**: A string containing the description for the account.
- **DomainName**: A string containing the domain name for the account.
- **DistinguishedName**: A string containing the distinguished name for the account.
- **Asset/Name**: A string containing the asset that contains this account.

AssetAccountPassword template

The AssetAccountPassword template CSV contains the following columns:

- **Name**: A string containing the name of the account to set the password on.
- **Asset/Name**: A string containing the name of the asset that contains this account.
- **Asset/AssetPartitionName**: A string containing the name of the partition of the asset that contains this account.
- **Password**: A string containing the password to set on this accout.

AssetAccountSshKey template

The AssetAccountSshKey template CSV contains the following columns:

- **Name**: A string containing the name of the account to set the SSH key on.
- **Asset/Name**: A string containing the name of the asset that contains this account.
- **Asset/AssetPartitionName**: A string containing the name of the partition of the asset that contains this account.
- **PrivateKey**: A string containing the Private Key.
- **Passphrase**: A string containing the passphrase to access the Private Key, blank if not needed.
- **Comment**: A string containing the SSH Key comment.

User template

The User template CSV contains the following columns:

- **Name**: A string containing the username to give to the new user.

  NOTE: Names must be unique per identity provider.
- **FirstName**: A string containing the first name of the user.
- **LastName**: A string containing the last name of the user.
- **Description**: A string containing the description of the user.
- **EmailAddress**: A string containing the email address of the user.
- **WorkPhone**: A string containing the work phone number of the user.
- **MobilePhone**: A string containing the mobile phone number of the user.
- **AdminRoles**: A string containing the permissions (admin roles) to assign to the user.

  Use the following format: `"[""permission"","permission"","permission""]"`

  The valid values are `GlobalAdmin`, `ApplicationAuditor`, `SystemAuditor`, `Auditor`, `AssetAdmin`, `ApplianceAdmin`, `PolicyAdmin`, `UserAdmin`, `HelpdeskAdmin`, `OperationsAdmin`.
- **DirectoryProperties/DomainName**: A string containing the DNS name of the domain this user is in.
- **PrimaryAuthenticationProvider/Name**: A string containing the name of the authentication provider.
- **PrimaryAuthenticationProvider/Identity**: A string containing the identity of the user to authenticate with.
- **Password**: A string containing the password.

Security Policy Management

In the web client, expand the **Security Policy Management** section in the left navigation pane.

Access Request Activity

The **Access Request Activity** page allows Security Policy Administrators to review and manage access requests from a single location. Clicking one of the access request tiles on the page displays additional information about the access requests belonging to that category. In addition, you can review the request workflow, launch a live session, end a session, or revoke a specific request.

This dashboard is available to SPP users assigned the following administrative permissions:

- Auditor: Read-only view.
- Security Policy: Full control.

Access requests: Tiles

Clicking any of the following tiles will open a dialog showing additional information. Click the button to customize the tiles that are displayed.

- **Open Requests**: Displays a list of all currently opened access requests, including session requests and password release requests.
- **Pending Approval**: Displays a list of access requests to be approved.
- **Pending Review**: Displays a list of access requests to be reviewed.
- **Open Sessions**: Displays a list of all currently opened sessions.
- **Passwords Out**: Displays a list of all password release requests that are currently checked out.
- **SSH Keys Out**: Displays a list of all SSH key release requests that are currently checked out.
- **API Keys Out**: Displays a list of all API key release requests that are currently checked out.

Access requests: Toolbars

After opening one of the tiles, use the toolbar at the top of the details grid to perform the following tasks.

- **View Details**: Select to view additional information regarding the request.
- **Request Workflow Details**: Select to review the transactions that took place in the selected request. Clicking this button displays the **Request Workflow** dialog allowing you to audit the transactions that occurred during the request's workflow from request to approval to review.
- **Session Audit Log in SPS**: Click this button to open the session audit log in Safeguard for Privileged Sessions.
- **View Live Session**: Select to view a live session for the selected session request. Clicking this button launches the Desktop Player (minimum version supported is 1.11.15) allowing you to follow an active session.

  For details on using the Desktop Player, go to One Identity Safeguard for Privileged Sessions - Technical Documentation. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.
- **Terminate Live Session**: Select to close the live session for the selected session request.
- **Close Request**: Select to retract the selected access request.
- **Export**: Select to create a .csv or .json file of the currently displayed access request grid and save it to a location of your choice. The time is set according to the user time zone.
- **Columns**: Select to display a list of columns that can be displayed in the grid. Select the check box for data to be included in the grid. Clear the check box for data to be excluded from the grid.

Account Groups

A SPP account group is a set of accounts which you can add to the scope of an access request policy. For more information, see Creating an access request policy.

The Auditor and the Security Policy Administrator have permission to access **Account Groups**.

To access **Account Groups**, in the web client, navigate to **Security Policy Management** > **Account Groups**.

The **Account Groups** view displays the following information about the selected account group.

- Properties tab (account group): Displays general information about the selected account group.
- Accounts tab (account group): Displays the accounts associated with the selected account group.
- Access Request Policies tab (account group): Displays the entitlements and access request policies associated with the selected account group.
- History tab (account group): Displays the details of each operation that has affected the selected account group.

Use these toolbar buttons to manage account groups.

- **+Account Group**: Add account groups to SPP. For more information, see Adding an account group on page 473..
- **+ Account Dynamic Group**: Add dynamic account groups to SPP. For more information, see Adding a dynamic account group on page 474..
- **Delete**: Remove the selected account group from SPP. For more information, see Deleting an account group on page 478..
- **View Details**: Used to display information and configuration options for the selected account group.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of account groups.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Properties tab (account group)

The **Properties** tab lists information about the selected Account Group.

To access **Properties**:

- web client: Navigate to **Security Policy Management** > **Account Groups** > (View Details) > **Properties**.

Table 181: Account Groups Properties tab: General properties

Property	Description
Name	The selected account group's name
Description	Information about the selected account group
Account Rules	For dynamic account groups, a summary of the asset account rules defined

Accounts tab (account group)

The **Accounts** tab displays the accounts associated with the selected account group.

To access **Accounts**, in the web client, navigate to **Security Policy Management** > **Account Groups** > ✎ **View Details** > **Accounts**.

Table 182: Account Groups: Accounts tab properties

Property	Description
Name	Name of the account belonging to the selected account group.
Parent	The asset to which the account belongs.
Domain Name	For directory accounts, the name of the domain the account is associated with.
Disabled	A check in this column indicates that the account is not managed.
Service Account	A check in this column indicates that the account is a service account.
Password Request	A check in this column indicates that password release requests are enabled for this account.
Session Request	A check in this column indicates that session access requests are enabled for this account.
SSH Key Request	A check in this column indicates that SSH key access requests are enabled for this account.
Password	A check in this column indicates that a password is set for the selected account. For more information, see Checking, changing, or setting an account password on page 291..
SSH Key	A check in this column indicates that an SSH key is set for the selected account. For more information, see Checking, changing, or setting an SSH key on page 292..
Description	Information about the account.

Use these buttons on the details toolbar.

Table 183: Account Groups: Access Request Policies tab toolbar

Option	Description
+ Add Account	To add one or more accounts to the account group you selected.
− Remove	Remove the selected account.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.

Option	Description
Refresh	Update the list of accounts.
Search	To locate a specific account in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78..

Access Request Policies tab (account group)

The **Access Request Policies** tab displays the entitlements and policies. These may include policies for password and SSH key release and session request policies that are associated with the selected account group.

To access **Access Request Policies**, in the web client, navigate to **Security Policy Management** > **Account Groups** > **View Details** > **Access Request Policies**.

Table 184: Account Groups: Access Request Policies tab properties

Property	Description
Entitlement	The name of the access request policy's entitlement.
Access Request Policy	The name of the policy that governs the accounts in the selected account group.
# Account Groups	The number of unique account groups in the access request policy.
# Accounts	The number of unique accounts in the account groups that are associated with the access request policy.

Use these buttons on the details toolbar to manage your access request policies associated with the selected account group.

Table 185: Account Groups: Access Request Policies tab toolbar

Option	Description
+ Add	Add the selected account group to the scope of one or more access request policy. Clicking this button displays the **Access Policies** dialog, allowing you to select a policy.
− Remove	Remove the selected account group from the scope of the selected access policy.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of access request policies.
Search	To locate a specific policy or set of policies in this list, enter the

Option	Description
	character string to be used to search for a match. For more information, see Search box on page 78..

History tab (account group)

The **History** tab allows you to view or export the details of each operation that has affected the selected account group.

To access **History**:

- web client: Navigate to **Security Policy Management** > **Account Groups** > (View Details) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
  - **Refresh**: Update the list displayed.
  - **Search**: For more information, see Search box on page 78.

Table 186: Account Groups: History tab properties

Property	Description
Date/Time	The date and time of the event.
User	The display name of the user that triggered the event.
Source IP	The network DNS name or IP address of the managed system that triggered the event.
Object Name	The name of the selected account group.
Event	The type of operation made to the selected account group: • Create • Delete • Update • Add Membership • Remove Membership

Property	Description
	NOTE: A membership operation indicates a relationship change with a related or parent object such as the selected account group was added or removed from the membership of a policy, or an account was added or removed from the membership of the selected account group.
Related Object	The name of the related object.
Related Object Type	The type of the related object.
Parent	The name of the object to which the selected account group is a child.
Parent Object Type	The parent object type.

Managing account groups

Use the controls and tabbed pages in the Account Groups view to perform the following tasks to manage SPP account groups:

- Adding an account group
- Adding a dynamic account group
- Adding one or more accounts to an account group
- Adding accounts to an access request policy
- Deleting an account group

Adding an account group

It is the responsibility of the Security Policy Administrator to add account groups to SPP.

To add an account group

1. Navigate to **Security Policy Management** > **Account Groups**.
2. Click **+ Add** > **Account Group** from the toolbar.
3. In the **New Account Group** dialog, enter the following information:
    - **Name**: Enter a unique name for the account group.

      Limit: 50 characters
    - **Description**: (Optional) Enter information about this account group.

      Limit: 255 characters
4. Click **OK**.

Adding a dynamic account group

It is the responsibility of the Security Policy Administrator to add dynamic account groups to SPP.

Dynamic account groups are associated with rules engines that run when pertinent objects are created or changed. For example:

- Whenever you add or change an asset account, all applicable rules are reevaluated against that asset account.
- Whenever you change an asset account rule, the rule is reevaluated against all asset accounts within the scope of that rule. In other words, the rule is reevaluated against all asset accounts for grouping and the asset accounts within the designated partitions for tagging.

You can create a dynamic account group without any rules; however, no accounts will be added to this dynamic account group until you have added a rule.

In large environments, there is a possibility that the user interface may return before all of the rules have been reevaluated and you may not see the results you were expecting. If this happens, wait a few minutes and **Refresh** the screen to view the results.

To add a dynamic account group

1. Navigate to **Security Policy Management** > **Account Groups**.
2. Click **+ Add** > **Account Dynamic Group** from the toolbar.
3. In the **New Account Group** dialog, provide information in each of the tabs:

Table 187: Information to provide when adding a dynamic account group

Tab	Information to provide
General tab (add dynamic account group)	Where you add general information about the dynamic account group.
Account Rules tab (add dynamic account group)	Where you define the rules to be used to identify the accounts to be included in a dynamic account group.

General tab (add dynamic account group)

On the **General** tab of the **Dynamic Account Group** dialog, supply general information about the dynamic account group.

Table 188: Dynamic Account Group: General tab

Property	Description
Name	Enter a unique name for the dynamic account group. Limit: 50 characters

Property	Description
Description	Enter information about this dynamic account group. Limit: 255 characters

Account Rules tab (add dynamic account group)

Use the rule editor controls on the **Account Rules** tab of the **Dynamic Account Group** dialog to define the accounts that are to be included in the dynamic account group.

Table 189: Dynamic Account Group: Asset Account Rules tab

Property	Description
Enable rule for this group	Select this check box to include an asset account rule for this dynamic account group. Selecting this check box enables the rule editor controls. NOTE: You can create a dynamic account group without any rules; however, no accounts will to added to this dynamic account group until you have added a rule.
AND | **OR**	Click **AND** to group multiple search criteria together where all criteria must be met in order to be included. Click **OR** to group multiple search criteria together where at least one of the criteria must be met in order to be included.
Attribute	In the first query clause box, select the attribute to be searched. Valid attributes include: • **Name** (Default) • **Description** • **Platform** • **Disabled** • **Tag** • **Service Account** • **Partition Name** • **Asset Name** • **Asset Tag** • **Domain Name** • **NETBIOS Name** • **Distinguished Name** (You cannot do a one-level search with this attribute.) • **SID**

Property	Description
	• **Discovered Group Name** (Use this selection to not specify the domain in the search. To specify the domain, select **Discovered Group Distinguished Name**.) • **Discovered Group Distinguished Name** (Use this selection to specify the search is for the domain to which the group belongs.) • **Directory Container** (If you use the operator **Equal**, one level is found.)
Operator	In the middle clause query box, select the operator to be used in the search. The operators available depend upon the data type of the attribute selected. For string attributes, the operators may include: • **Contains** (Default) • **Does Not Contain** • **Starts With** • **Ends With** • **Equals** • **Does Not Equal** • **Matches** For boolean attributes (such as Service Account), the operators may include: • Is **True** • Is **False**
Enter condition value	In the last clause query box, enter the search string or value to be used to find a match. If you selected an attribute of **Discovered Group Name**, **Discovered Group Distinguished Name**, or **Directory Container**: 1. Click **Browse** to go to the **Select Directory Asset to Search** dialog to locate the search string. The **Name**, **Asset Partition**, and **Description** for each directory display. 2. Choose a directory and click **OK**. 3. On the **Location** dialog, select the location and click **OK**.
+ | −	Click + to the left of a search clause to add an additional clause to the search criteria. Click − to remove the search clause from the search criteria.

Property	Description
Add Grouping | **Remove**	Click the + **Add Grouping** button to add an additional set of conditions to be met. A new grouping is added under the last query clause in a group and appears in a bordered pane, showing that it is subordinate to the higher-level query conditions. Click the **Remove** button to remove a grouping from the search criteria.
Preview	Click **Preview** to run the query in order to review the results of the query before adding the dynamic group.

Adding one or more accounts to an account group

From the **Account Groups** view, you can add one or more accounts to an account group.

To add accounts to an account group

1. Navigate to **Security Policy Management** > **Account Groups**.
2. Select an account group and click **View Details**.
3. Open the **Accounts** tab.
4. Click + **Add Account**.

   NOTE: If you do not see the account you are looking for, depending on your Administrator permissions, you can create it in the **New Account** dialog (accessed via the + **New Account** button). (You must have Asset Administrator permissions to create accounts.)
5. Select one or more accounts from the list in the **Select accounts to add to group** dialog.
6. Click **Select Accounts** to save your selections.

Adding accounts to an access request policy

To add accounts to an access request policy

1. Navigate to **Security Policy Management** > **Account Groups**.
2. In **Account Groups**, select an account group from the object list and open the **Access Request Policies** tab.
3. Click + **Add** from the details toolbar above the grid.
4. Select a policy from the list in the **Access Policies** dialog and click **OK**.

Deleting an account group

When you delete an account group, SPP does not delete the associated accounts.

To delete an account group

1. Navigate to **Security Policy Management** > **Account Groups**.
2. In **Account Groups**, select an account group from the object list.
3. Click **Delete**.
4. Confirm your request.

Application to Application

In order for third-party applications to use the Application to Application service to integrate with the SPP vault, you must first register the application in SPP. This can be done using the **Security Policy Management** > **Application to Application** page described below. Once the application is registered, you can enable or disable the service. For more information, see Global Services.

Application to Application displays a list of previously registered third-party applications. From this page, the Security Policy Administrator can add new application registrations, and modify or remove existing registrations. The **Application to Application** page displays the following details about application registrations.

Table 190: Application to Application: Properties

Property	Description
Name	The name assigned to the application's registration.
Certificate User	The name of the certificate user associated with the registered application. NOTE: If there is no certificate user listed for an application registration, contact your Security Policy Administrator to add one. The Application to Application service on the third-party application will not work with the SPP vault until a certificate user has been specified.
Enable/Disable Toggle on Toggle off	Indicates whether the application registration is enabled. The toggle appears blue with the switch to the right when the service is enabled, and gray with the switch to the left when the service is disabled. Click the toggle to enable or disable an application registration. NOTE: When an application registration is disabled, Application to Application access is disabled for that third-party application until the registration is enabled again.
Description	Information about the application's registration.

Use these toolbar buttons to manage application registrations.

Table 191: Application to Application: Toolbar

Option	Description
Add	Add an application registration to SPP. For more information, see Adding an application registration on page 481.
Remove	Remove the selected application registration from SPP. For more information, see Deleting an application registration on page 483.
Refresh	Update the list of application registrations.
Edit	Modify the selected application registration.

About Application to Application functionality

Using the Application to Application service, third-party applications can interact with SPP in the following ways:

- Credential retrieval: A third-party application can retrieve a credential from the SPP vault in order to perform automated functions on the target asset. In addition, you can replace hard coded passwords in procedures, scripts, and other programs with programmatic calls.
- Access request broker: A third-party application can initiate an access request on behalf of an authorized user so that the authorized user can be notified of the available request and log in to SPP to retrieve a password or start a session.

NOTE: If Offline Workflow Mode is triggered, Application to Application operations will be halted for the number of minutes it takes to move to Offline Workflow Mode. For more information, see About Offline Workflow Mode on page 581..

Credential retrieval

A credential retrieval request using the Application to Application service allows the third-party application to retrieve credentials from the SPP vault without having to go through the normal workflow process.

For example, say you have an automated system that performs a routine system diagnostic on various services in the data center every 24 hours. In order for the automated system to perform the diagnostics, it must first authenticate to the target server. Since all of the credentials for the target servers are stored in the SPP vault, the automated system retrieves the credentials for a specified system by calling the Application to Application service.

Access request broker

An access request broker request using the Application to Application service allows the application to create an access request on behalf of another user.

For example, say you have a ticketing system and one of the types of tickets that can be created is to request access to a specific asset. The ticketing system can be integrated with SPP through the Application to Application service to create an access request on behalf of the user that entered the ticket into the system. Once the request is created, it follows the normal access request workflow in SPP and the user who entered the ticket will be notified when access is granted.

In order for a third-party application to perform one of tasks provided by the Application to Application service, the application must first be registered with SPP. This registration will be associated with a certificate user and authentication to the Application to Application service will be done using the certificate and an API key. The registered application will not be allowed to authenticate to SPP other than for the purpose specified. The properties associated with an application registration are:

- **API key**: As part of the registration process, an API key is generated. An administrator must then copy this API key and make it available to the third-party application.
- **Certificate user**: In addition to the API key, the application registration must be associated with a certificate user. The certificate that is associated with the certificate user must be signed by a certificate authority that is also trusted by SPP.

  NOTE: Use your corporate PKI for issuing this certificate and installing it on the third-party application.

The Application to Application service is disabled by default and must be enabled before any credential retrievals or access request broker functions can be performed.

Using the web client:

1. Navigate to **Security Policy Management** > **Application to Application**.
2. In the **Enabled** column for the service, move the toggle to the right to enable the service.

Using the API, use the following URL:

`https://appliance/service/appliance/v4/A2AService/Enable`

In addition, you can check the current state of the service using the following URL:

`https://appliance/service/appliance/v4/A2AService/Status`

Setting up Application to Application

In order to use Application to Application integration with SPP, you must perform the following tasks:

1. Prepare third-party application for integration with SPP.
2. Appliance Administrator enables Application to Application service in SPP. Use one of the following methods:
   - Using the web client, navigate to **Security Policy Management** > **Application to Application**. In the **Enabled** column for the service, move the toggle to the right to enable the service.
   - Use the following URL: `https://appliance/service/appliance/v4/A2AService/Enable`.
3. Asset Administrator adds assets and accounts to SPP. For more information, see Adding an asset and Adding an account
4. User Administrator adds certificate users to SPP. For more information, see Adding a user on page 541.
5. Security Policy Administrator adds application registration to SPP. For more information, see Adding an application registration on page 481.
6. Get the API key and copy/paste it into the third-party application in order to make requests from the third-party application. For more information, see Making a request using the Application to Application service on page 484.

Adding an application registration

To allow a third-party application to perform one of the tasks provided by the Application to Application service, you must register the third-party application with SPP.

Prerequisites

- User Administrator adds certificate users to SPP.
- Asset Administrator adds assets and accounts to SPP.

To add an application registration

1. Log in to the SPP web client as a Security Policy Administrator.
2. Navigate to **Security Policy Management** > **Application to Application**.
3. Click **+Add**. The **New Registration** dialog displays.
4. Specify the following information:
   a. **Name**: Enter a name for the application registration.
   b. **Description**: Enter information about the application registration.
   c. **Certificate User**: Click **Browse** to select a certificate user who is associate with the third-party application being registered.

A certificate user must be specified. If not specified when you initially add an application registration, click ✎**Edit** on the **Application to Application** page to specify the certificate user.

> NOTE: For SignIR, connect as a certificate user using A2A API key for the retrievable account you want to monitor that is assigned an A2A registration for Retrievable Accounts. The connected certificate user will receive event notifications for any events related to that account (for example, password change, update, and delete). For more information, see Making a request using the Application to Application service on page 484.

d. **Visible To Certificate Users**: Select this check box to make the registration, including the API keys, visible by the certificate user that is configured for the A2A registration.

5. Click **OK**. This will save the initial application registration information and open a new dialog with additional settings.
6. The **Access Request Broker** tab displays a list of users for which the third-party application can create an access request on behalf of.
   - Click **+** to add a user or user group to the list.
   - Click **Edit Restrictions** to specify IP address restrictions for all of the users and user groups in the list.

     A restriction is a list of IP addresses or range of IP addresses that are allowed to call the Application to Application service to perform this task. That is, if a restriction is added to a Credential Retrieval or Access Request Broker task, the service will only allow requests that initiate from the IP addresses specified in the restriction list.

     The IP address notation can be:
     - An IPv4 or IPv6 address (for example, 10.5.32.4).
     - An address range in CIDR notation (for example, 10.5.0.0/16).
   - Click **−** to remove the selected user from the list.
7. The **Credential Retrieval** tab displays a list for which the third-party can retrieve credentials from SPP without going through the normal workflow process.
   - Click **+** to add an account to the list.
   - Click **Restrictions** in the Restrictions column to specify IP address restrictions for the selected account.

     A restriction is a list of IP addresses or range of IP addresses that are allowed to call the Application to Application service to perform this task. That is, if a restriction is added to a Credential Retrieval or Access Request Broker task, the service will only allow requests that initiate from the IP addresses specified in the restriction list.

     The IP address notation can be:

    - An IPv4 or IPv6 address (for example, 10.5.32.4).
    - An address range in CIDR notation (for example, 10.5.0.0/16).
  - Click − to remove the selected account from the list.
8. Click **OK** to save and close the dialog.

Once an application registration is added to SPP, the third-party application can authenticate with SPP using the API key that was generated and the certificate that was associated with the registration. To make a request, you must retrieve the relevant API key for the application using an authorized account (that is, using bearer token authentication) and install the correct certificate on the host that will make the request. For more information, see Making a request using the Application to Application service on page 484.

Deleting an application registration

You can delete a previously configured application registration from SPP.

To delete an application registration

1. Navigate to **Security Policy Management** > **Application to Application**.
2. Select the application registration to be deleted.
3. Click the 🗑 toolbar button.
4. Confirm your request.

Regenerating an API key

If, as the Security Policy Administrator, you discover that the API key has been stolen or misplaced, you can regenerate the API key at any time. When you regenerate an API key, it invalidates the old API key and prevents any services from using that key to access the Application to Application service.

To regenerate an API key

1. Log in to the SPP web client as a Security Policy Administrator.
2. Navigate to **Security Policy Management** > **Application to Application**.
3. Select an application registration from the list and click (Edit).
4. On the Access Request Broker tab, click (Regenerate).

You can now view or copy the new API key to the clipboard and use this new API key in your third-party application to access the Application to Application interfaces. See Making a request using the Application to Application service.

Making a request using the Application to Application service

Using the Application to Application service, third-party applications can interact with SPP in the following ways:

- Credential retrieval: A third-party application can retrieve a credential from the SPP vault in order to perform automated functions on the target asset. In addition, you can replace hard coded passwords in procedures, scripts, and other programs with programmatic calls.
- Access request broker: A third-party application can initiate an access request on behalf of an authorized user so that the authorized user can be notified of the available request and log in to SPP to retrieve a password or start a session.

A third-party application authenticates with SPP using an API key and a client certificate, rather than the bearer token normally used to authenticate SPP API requests. To make a request, you must first retrieve the API key for the application from SPP using an authorized user account (that is, using bearer token authentication), and install the correct certificate on the host that will be making the request. The certificate must be installed in the certificate store of the authorized certificate user that will make the request.

Prerequisites

- Register the third-party application with SPP. For more information, see Adding an application registration on page 481.
- Associate the third-party application with an existing SPP certificate user.

To make a credential retrieval request from the third-party application

1. Retrieve the relevant API key for the application from SPP. You can retrieve the API key using the following methods:

   Using the web client:

   - Log in to the SPP client as a Security Policy Administrator.
   - Navigate to **Security Policy Management** > **Application to Application**.
   - Select the application and click (Edit).
   - On the **Credential Retrieval** tab, click .

   Using the SPP API:

   - Use the following URL to retrieve the details of the registered application from the SPP API. The ID property in the response can then be used to retrieve the relevant API key. The Certificate Thumbprint property in the response identifies the certificate that the application must use to authentication the request.

```
https://<ApplianceIP>/service/core/v4/A2ARegistrations?filter=AppName%20eq%20%22<ApplicationName>%22
```

- Use the ID property in the response retrieved for the application registration to retrieve the API key for the selected account from the SPP API.

```
https://<Appliance IP>/service/core/v4/A2ARegistrations/<AppId>/RetrievableAccounts?filter=AssetName%20eq%20%22<Asset Name>%22%20and%20AccountName%20eq%20%22<AccountName>%22
```

2. Ensure that the certificate matching the application's registered CertificateUserThumbprint is installed on the host that will be making the request.
3. Ensure that the selected certificate is trusted by SPP. That is, install the trusted root certificate in SPP.
4. Create the application request, authenticating with the retrieved API key and the certificate thumbprint.
   - Set the Authorization header in the request to `A2A <API key>`.
   - The type can be `Password` or `PrivateKey`. Note that private keys can only be retrieved for service accounts.
   - Present the certificate with the request as appropriate for the invoking method. For example, when using the `Invoke-WebRequest` cmdlet, use the option:

     ```
     -CertificateThumbprint <thumbprint>
     ```

     To retrieve a credential, use the following request:

     ```
     GET https://<ApplianceIP>/service/A2A/v4/Credentials?type=Password
     Host: <ApplianceIP>
     Content-Type: application/json
     Accept: text/plain
     Authorization A2A <API Key>
     ```

     This URL returns a string response.

To make an access request broker request from the third-party application

1. Retrieve the relevant API key for the application from SPP. You can retrieve the API key using the following methods:

   Using the web client:

   - Log in to the SPP client as a Security Policy Administrator.
   - Navigate to **Security Policy Management** > **Application to Application**.
   - Select the application and click (Edit).
   - On the **Access Request Broker** tab, click .

   Using the SPP API:

   - Use the following URL is retrieve the details of the registered application from the SPP API. The Id property in the response can then be used to retrieve the

relevant API key. The Certificate Thumbprint property in the response identifies the certificate that the application must use to authentication the request.

```
https://<ApplianceIP>/service/core/v4/A2ARegistrations?filter=AppName%20eq%20%22<ApplicationName>%22
```

- Use the ID retrieved for the application registration to retrieve the API key from the Safeguard API:

```
https://<Appliance IP>/service/core/v4/A2ARegistrations/<Id>/AccessRequestBroker/ApiKey
```

2. Ensure that the certificate matching the application's registered `CertificateUserThumbprint` is installed on the host that will be making the request.
3. Ensure that the selected certificate is trusted by SPP. That is, install the trusted root certificate in SPP.
4. Create the application request, authenticating with the retrieved API key and the certificate thumbprint.
   - Set the Authorization header in the request to `A2A <API key>`.
   - Present the certificate with the request as appropriate for the invoking method. For example, when using the `Invoke-WebRequest` cmdlet, use the option:

     ```
     -CertificateThumbprint <thumbprint>
     ```

   - To create an access request, use the following request:

     ```
     POST
     Host: <Appliance IP>
     Accept            application/json
     Content-type      application/json
     Authorization     A2A <API key>
     {
          "ForUser": "<user name>",
          "ForUserId": <user id>,
          "ForProvider": “<providername>”,
     "SystemId": <system id>,
          "SystemName": "<system name>",
          "AccountId": <account id>,
          "AccountName": "<account name>",
          "AccessRequestType": "<request type>",
     “RequestedDurationDays”: <days>
          "RequestedDurationHours": <hours>,
     “RequestedDurationMinutes”: <minutes>,
     “RequestedFor”: “<date>,
          "ReasonCodeId": <reason code id>,
          "ReasonCode": "<reason name>",
          "ReasonComment": "<reason comment>",
     “IsEmergency”: <bool>,
     “TicketNumber”: “<ticket>”

     }
     ```

     This URL returns the new request if successful.

Exceptions

Most of the fields in this access request match those in a normal access request, with the exceptions noted here:

The following fields are used to identify the target SPP user that will be used to create the request. The result must uniquely identify a valid SPP user for which the application has been granted permission to create an access request. If the search results in multiple matches or no matches, an error is returned.

- ForUserId: The database ID of a SPP user. This takes priority if it contains a value.
- ForUser: The name of a SPP user. This value is ignored if ForUserId contains a value.
- ForProvider: An optional provider name, that can be used to limit the search for ForUser.

The following fields are used to uniquely identify the target system. If the search results in multiple matches or no matches, an error is returned.

- SystemId: The database ID of a SPP asset. This field is used to search for a matching asset in the following order:
    - System Name: Exact match on the system name
    - Network Address: Exact match on the network address
    - String search: A string search on all string properties for the asset

The following fields are used to uniquely identify the target account. If the search results in multiple matches or no matches, an error is returned.

- AccountId: The database ID of a SPP account. This takes priority if it contains a value.
- AccountName: This is ignored if AccountId contains a value. This field is used to search for a matching account in the following order:
    - Account Name: Exact match on the account name
    - String search: A string search on all string properties for the account

The following fields can be used to identify the reason code. If the search results in multiple matches or no matches, the reason code is set to null.

- ReasonCodeId: The database ID of a predefined reason code. This takes priority if it contains a value.
- ReasonCode: The name of a predefined reason code. This is ignored if ReasonCodeId contains a value.

Access request creation

Once the target user and account have been determined, the Application to Application service attempts to create the access request. Normal policy rules determine whether the attempt is successful.

Cloud Assistant

The Cloud Assistant feature integrates its access request workflow with Starling Cloud Assistant, allowing approvers to receive a notification through a configured channel when an access request is submitted. The approver can then approve (or deny) access requests through the channel without needing access to the SPP web application.

The Cloud Assistant feature is enabled when you join SPP to Starling. For more information, see Starling on page 229. Once enabled, it is the responsibility of the Security Policy Administrator to define the users who are authorized to use Cloud Assistant to approve access requests.

Go to Cloud Assistant:

- web client: Navigate to **Security Policy Management** > **Cloud Assistant**.

The **Cloud Assistant** pane displays the following about the users authorized to use the feature.

Table 192: Cloud Assistant: Properties

Setting	Description
Name	Name of the SPP user. NOTE: This user must also be added as an approver in an access request policy.
Username	The username associated with the account.
Authentication Provider	The type of authentication provider.
Identity Provider	The name of the authentication provider for the account.
Domain Name	The name of the domain where the account it located.
Email Address	Valid email address for the authorized user.

Use these toolbar buttons to manage the users authorized to use Cloud Assistant.

Table 193: Cloud Assistant: Toolbar

Setting	Description
+ **Add**	Add SPP users who are authorized to use this feature to approve (or deny) access requests. NOTE: These same users must also be added as approvers in an access request policy.
− **Remove**	Remove the selected user as an authorized user.
Refresh	Update the list of users authorized to use Cloud Assistant.

Adding authorized user for Cloud Assistant

Once SPP is joined to Starling, use the **Cloud Assistant** page to add the SPP users that can use the Cloud Assistant feature to approve access requests.

To add users who are authorized to use Cloud Assistant

IMPORTANT: The user information configured in SPP must match the user information in the Starling Cloud Assistant channel. If the user information does not match, you will need to remove the user from both **Security Policy Management** > **Cloud Assistant** and Starling Cloud Assistant's **Recipients** page, then re-add the user to SPP using the correct user information.

1. Log in to the SPP client as a Security Policy Administrator.
2. To go to Cloud Assistant:
   - web client: **Security Policy Management** > **Cloud Assistant**.
3. Click **+ Add**.
4. In the **Users** dialog, select users from the list and click **OK**.
5. Add these Cloud Assistant users as approvers in the appropriate access request policy. For more information, see Creating an access request policy.

Once a user is added as a Cloud Assistant user and as an approver in an access request policy, when an access request requires approval, SPP sends a notification to the approver's configured channel (this is configured via the Starling Cloud Assistant service). The approver can either approve or deny the access request directly from the channel.

NOTE: Revoking an access request that has already been approved is not available via the channel. You must use the SPP web client to perform that action.

Asset Groups

A SPP asset group is a set of assets that you can add to the scope of an access request policy. For more information, see Creating an access request policy.

Only the assets that support session management can be added to asset groups and dynamic asset groups. Assets that do not support session management include but may not be limited to Directory assets. When you create the asset, the **Management** tab has an **Enable Session Request** check box if sessions is supported. For more information, see Supported platforms on page 33. This section lists SPP and Safeguard for Privileged Sessions support by platform.

The Auditor and the Security Policy Administrator have permission to access **Asset Groups**.

To access **Asset Groups**:

- web client: Navigate to **Security Policy Management** > **Asset Groups**.

The **Asset Groups** view displays the following information about the selected asset group.

- Properties tab (asset group): Displays general information about the selected asset group. For dynamic groups, Asset Rules information is also displayed under this tab.
- Assets tab (asset group): Displays the assets associated with the selected asset group.
- Access Request Policies tab (asset group): Displays the entitlements and access request policies associated with the selected asset group.
- History tab (asset group): Displays the details of each operation that has affected the selected asset group.

Use these toolbar buttons to manage asset groups.

- **New Asset Group** > **Asset Group**: Add asset groups to SPP. For more information, see Adding an asset group on page 494.
- **New Asset Group** > **Asset Dynamic Group**: Add dynamic asset groups to SPP. For more information, see Adding a dynamic asset group on page 495.
- **Delete**: Remove the selected asset group from SPP. For more information, see Deleting an asset group on page 498.
- **View Details**: Used to display information and configuration options for the selected asset group.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of asset groups.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Properties tab (asset group)

The **Properties** tab lists information about the selected asset group.

To access the **Properties** tab, in the web client, navigate to **Security Policy Management** > **Asset Groups** > **View Details** > **Properties**.

Table 194: Asset Groups Properties tab: General properties

Property	Description
Name	The selected asset group's name

Property	Description
Description	Information about the selected asset group
Asset Rules	For dynamic asset groups, a summary of the asset rules defined. On the web client, this information is available on the **Asset Rules** tab.

Assets tab (asset group)

The **Assets** tab displays the assets associated with the selected asset group.

To access **Assets**:

- web client: Navigate to **Security Policy Management** > **Asset Groups** > (View Details) > **Assets**.

Click **+ Add Asset** from the details toolbar to add one or more assets to the selected asset group.

Search: For more information, see Search box on page 78.

Table 195: Asset Groups: Assets tab properties

Property	Description
Name	The asset name assigned to the managed system.
Platform	The platform of the managed system.
Session Request	A check in this column indicates that session access requests are enabled for the asset.
Disabled	A ✓ check in this column indicates that the asset is not managed, is disabled, and has no associated accounts.
Description	Information about the asset.

Use these buttons on the details toolbar.

Table 196: Asset Groups: Assets tab toolbar

Option	Description
+ Add Asset	To add one or more assets to the asset group you selected.
— Remove	Remove the selected asset.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.

Option	Description
Refresh	Update the list of assets.
Search	To locate a specific asset in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Access Request Policies tab (asset group)

The **Access Request Policies** tab displays the entitlements and access request policies associated with the selected asset group.

To access **Access Request Policies**:

- web client: Navigate to **Security Policy Management** > **Asset Groups** > (View Details) > **Access Request Policies**.

Table 197: Asset Groups: Access Request Policies tab properties

Property	Description
Entitlement	The name of the access request policy's entitlement.
Access Request Policy	The name of the policy that governs the assets in the selected asset group.
# Asset Groups	The number of unique asset groups in the access request policy.
# Assets	The number of unique assets in the asset groups that are associated with the access request policy.

Use these buttons on the details toolbar to manage your access request policies associated with the selected asset group.

Table 198: Asset Groups: Access Request Policies tab toolbar

Option	Description
Add	Add the selected asset group to the scope of an access request policy.
Remove	Remove the selected policy. For more information, see Deleting an access request policy on page 517.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of access request policies.

Option	Description
Search	To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

History tab (asset group)

The **History** tab allows you to view or export the details of each operation that has affected the selected asset group.

To access **History**:

- web client: Navigate to **Security Policy Management** > **Asset Groups** > (View Details) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
  - **Refresh**: Update the list displayed.
  - **Search**: For more information, see Search box on page 78.

Table 199: Asset Groups: History tab properties

Property	Description
Date/Time	The date and time of the event.
User	The display name of the user that triggered the event.
Source IP	The network DNS name or IP address of the managed system that triggered the event.
Object Name	The name of the selected asset group.
Event	The type of operation made to the selected account group: • Create • Delete • Update • Add Membership • Remove Membership

Property	Description
	NOTE: A membership operation indicates a "relationship" change with a related or parent object such as the selected asset group was added or removed from the membership of a policy, or an asset was added or removed from the membership of the selected asset group.
Related Object	The name of the related object.
Related Object Type	The type of the related object.
Parent	The name of the object to which the selected asset group is a child.
Parent Object Type	The parent object type.

Managing asset groups

Use the controls and tabbed pages in the Asset Groups view to perform the following tasks to manage SPP asset groups:

- Adding an asset group
- Adding a dynamic asset group
- Adding assets to an asset group
- Deleting an asset group

Adding an asset group

It is the responsibility of the Security Policy Administrator to add asset groups to SPP.

Use the **Asset Groups** view to add new asset groups to SPP.

Only the assets that support session management can be added to asset groups and dynamic asset groups. Assets that do not support session management include but may not be limited to Directory assets. When you create the asset, the **Management** tab has an **Enable Session Request** check box if sessions is supported. For more information, see Supported platforms on page 33. This section lists SPP and Safeguard for Privileged Sessions support by platform.

To add an asset group

1. Navigate to **Security Policy Management** > **Asset Groups**.
2. Click **+ Add**.
3. Click **+ Asset Group** from the drop-down.

4. In the **New Asset Group** dialog, enter the following information:
    a. **Name**: Enter a unique name for the asset group.

       Limit: 50 characters
    b. **Description**: (Optional) Enter descriptive text about this asset group.

       Limit: 255 characters
5. Click **OK**.

Adding a dynamic asset group

It is the responsibility of the Security Policy Administrator to add asset groups to SPP.

Only the assets that support session management can be added to asset groups and dynamic asset groups. Assets that do not support session management include but may not be limited to Directory assets. When you create the asset, the **Management** tab has an **Enable Session Request** check box if sessions is supported. For more information, see Supported platforms on page 33. This section lists SPP and Safeguard for Privileged Sessions support by platform.

To add a dynamic asset group

1. Navigate to **Security Policy Management** > **Asset Groups**.
2. From **Asset Groups**, click **+ Add** > **Add Asset Dynamic Group** from the toolbar.
3. In the **New Asset Group** dialog, provide information in each of the tabs.

Table 200: Information to provide when adding a dynamic asset group

Tab	Information to provide
General tab (add dynamic asset group)	Where you add general information about the dynamic asset group.
Asset Rules tab (add dynamic asset group)	Where you define the rules to be used to identify what assets are to be included in the dynamic asset group.

Related Topics

When does the rules engine run for dynamic grouping and tagging

General tab (add dynamic asset group)

On the **General** tab of the **New Asset Group** dialog, supply general information about the dynamic asset group.

Table 201: Dynamic Asset Group: General tab

Property	Description
Name	Enter a unique name for the dynamic asset group. Limit: 50 characters
Description	Enter information about this dynamic asset group. Limit: 255 characters

Asset Rules tab (add dynamic asset group)

Use the rule editor controls on the **Asset Rules** tab of the **New Asset Group** dialog to define what assets are to be included in the dynamic asset group.

Table 202: Dynamic Asset Group: Asset Rules tab

Property	Description
AND | **OR**	Click **AND** to group multiple search criteria together; where all criteria must be met in order to be included. Click **OR** to group multiple search criteria together; where at least one of the criteria must be met in order to be included.
Attribute	In the first query clause box, select the attribute to be searched. Valid attributes include: • **Name** (default) • **Description** • **Platform** • **Disabled** • **Tag** • **Discovery Job Name** • **Partition Name** • **Profile** • **Network Address** • **Discovered Group Name** (Use this selection to not specify the domain in the search. To specify the domain, select **Discovered Group Distinguished Name**.) • **Discovered Group Distinguished Name** (Use this selection to specify the search is for the domain to which the group belongs.)

Property	Description
	• **Directory Container** (If you use the operator **Equal**, one level is found.)
Operator	In the middle clause query box, select the operator to be used in the search. The operators available depend on the data type of the attribute selected. For string attributes, the operators may include: • Contains (Default) • Does not contain • Starts with • Ends with • Equals • Not equal For boolean attributes, the operators may include: • Is True • Is False
Search string	In the last clause query box, enter the search string or value to be used to find a match.
+ | −	Click + to the left of a search clause to add an additional clause to the search criteria. Click − to remove the search clause from the search criteria.
Add Grouping | **Remove**	Click the **Add Grouping** button to add an additional set of conditions to be met. A new grouping is added under the last query clause in a group and appears in a bordered pane, showing that it is subordinate to the higher level query conditions. Click the **Remove** button to remove a grouping from the search criteria.
Preview	Click **Preview** to run the query in order to review the results of the query before adding the dynamic group.

Adding assets to an asset group

From the **Assets** tab on the **Asset Groups** view, you can add one or more assets to an asset group.

To add assets to an asset group

1. Navigate to **Security Policy Management** > **Asset Groups**.
2. Select an asset group and click **View Details**.
3. Open the **Assets** tab.
4. Click **+ Add Asset**.
5. Select one or more assets from the list in the **Select assets to add to groups** dialog.

   NOTE: Only assets whose platform supports sessions management will be available.

   NOTE: If you do not see the asset you are looking for, depending on your Administrator permissions, you can create it in the **New Asset** dialog (accessed via the **+ New Asset** button). (You must have Asset Administrator permissions to create assets.)
6. Click **Select Assets** to save your selections.

Deleting an asset group

You can delete an asset group. When you delete an asset group, SPP does not delete the associated assets.

To delete an asset group

1. Navigate to **Security Policy Management** > **Asset Groups**.
2. In **Asset Groups**, select an asset group from the object list.
3. Click **Delete**.
4. Confirm your request.

Entitlements

A SPP entitlement is a set of access request policies that restrict system access to authorized users. Typically, you create entitlements for various job functions; that is, you assign permissions to perform certain operations to specific roles such as Help Desk Administrator, Unix Administrator, or Oracle Administrator. Password and SSH key release entitlements consist of users, user groups, and access request policies. Session access request entitlements consist of users, user groups, assets, asset groups, and access request policies. API Key release entitlements consist of accounts and account groups.

The Auditor and the Security Policy Administrator have permission to access **Entitlements**. An administrator creates an entitlement, then creates one or more access request policies associated with the entitlement, and finally adds users or user groups.

Go to Entitlements:

- web client: Navigate to **Security Policy Management** > **Entitlements**

If there are one or more invalid or expired policies, a ⚠ **Warning** and message (for example, `Entitlement contains at least one invalid policy`) displays. Go to the Access Request Policy tab to identify the invalid policy. For more information, see Access Request Policies tab (entitlements) on page 501.

The **Entitlements** view displays the following information:

- General tab (entitlements): Displays the general and time restriction settings information for the selected entitlement.
- Users tab (entitlements): Displays the user groups or users who are authorized to request access to the accounts or assets in the scope of the selected entitlement's policies. Certificate users are included in the display if the user was created during a Safeguard for Privileged Sessions link and was assigned and used by a Sessions Appliance. The certificate users created during the link can be added to the **Users** tab but are not there by default.
- Access Request Policies tab (entitlements): Displays the access request policies that govern the accounts or assets in the selected entitlement, including session access policies.
- History tab (entitlements): Displays the details of each operation that has affected the selected entitlement.

Use these toolbar buttons to manage entitlements.

- **New Entitlement**: add entitlements to SPP. For more information, see Adding an entitlement.
- **Delete**: Remove the selected entitlement. For more information, see Deleting an entitlement on page 518.
- **Edit**: Select an entitlement then click this button to open additional information and options for the asset.
- **Create a New Entitlement from the Selected Row**: Select an entitlement then click this button to duplicate the entitlement.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of entitlements.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

General tab (entitlements)

To access **General**:

- web client: Navigate to **Security Policy Management** > **Entitlements** > + (New Entitlement) or (Edit) > **General**.

The **General** tab lists information about the selected entitlement.

- **Name**: The entitlement name.
- **Description**: Information about the selected entitlement.
- **Priority**: A unique number that determines the processing order of the entitlement in relation to other entitlements. For more information, see How SPP evaluates policy when a user submits an access request on page 505.
- **Have the Entitlement Expire on Date and Time**: Select this option to enforce an expiration date, then enter the date and time.

  When an entitlement expires, all the access request policies associated with the entitlement also expire. To set an expiration date on a policy, see Creating an access request policy.
- **Use Time Windows**: Select this option to enforce time windows.

  Select and drag to highlight the hours you want to allow. Colored tiles are blocked times. Clear are available times.

Users tab (entitlements)

The **Users** tab displays the users and user groups who are authorized to request access for the accounts and assets in the scope of the selected entitlement's policies. Certificate users are included in the display if the user was created during a Safeguard for Privileged Sessions link and was assigned and used by a Sessions Appliance. The certificate users created during the link can be added to the **Users** tab but are not there by default.

To access **General**:

- web client: Navigate to **Security Policy Management** > **Entitlements** > (edit) > **Users**.

Click **+Add Users or Add User Groups** from the details toolbar to add one or more requester users or user groups to the selected entitlement.

Table 203: Entitlements: User tab properties

Property	Description
Type	Type of member:

Property	Description
	• Group • User
Display Name	Display name of the user or user group included in the selected entitlement.
Username	Name of the user or user group included in the selected entitlement.
Provider	The name of the authentication provider: • Local • Certificate • The name of an external provider such as a Microsoft Active Directory domain name.

Use these buttons on the details toolbar to manage the requester users associated with the selected entitlement.

Table 204: Entitlements: Users tab toolbar

Option	Description
Add Users or Add User Groups	Add a requester user group or requester user to the entitlement. For more information, see Adding users or user groups to an entitlement on page 517.
Delete	Remove the selected user or user group from the entitlement.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Search (case sensitive)	To locate a specific user (or user group) or set of users (or user groups) in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Access Request Policies tab (entitlements)

The **Access Request Policies** tab displays the password and SSH key request policies that govern the accounts in the selected entitlement.

To access **Access Request Policies**:

- web client: Navigate to **Security Policy Management** > **Entitlements** > (Edit) > **Access Request Policies**.

IMPORTANT: The selection made on the **Entitlement** > **Access Request Policy** tab takes precedence over the selections on **Appliance Management** > **Cluster** > **Managed Networks** page. If a **Managed Networks** rule includes nodes from different Safeguard for Privileged Sessions clusters, Safeguard for Privileged Passwords will only select the nodes from the same cluster that was assigned on the **Session Settings** page of the **Access Request Policy** tab.

Click **+New Access Policy** from the details toolbar to add a policy to the selected entitlement.

Use these buttons on the details toolbar to manage your access request policies.

Table 205: Entitlements: Access Request Policies tab toolbar

Option	Description
+New Access Policy	Add an access request policy to the selected entitlement. For more information, see Creating an access request policy.
Delete	Remove the selected policy from the selected entitlement. For more information, see Deleting an access request policy on page 517.
Edit	Modify the selected policy. For more information, see Modifying an access request policy on page 518.
Create a New Access Policy from the Selected Row	Make a copy of the selected policy. For more information, see Copying an access request policy on page 518.
Import Access Policies from Other Entitlements	Import an access policy that was configured for a different entitlement.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Search (case insensitive)	To locate a specific policy or set of policies in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

History tab (entitlements)

The **History** tab allows you to view or export the details of each operation that has affected the selected entitlement.

To access **History**:

- web client: Navigate to **Security Policy Management** > **Entitlements** > (Edit) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
  - **Refresh**: Update the list displayed.
  - **Search**: For more information, see Search box on page 78.

Table 206: Entitlements: History tab properties

Property	Description
Date/Time	The date and time of the event.
User	The display name of the user that triggered the event.
Source IP	The network DNS name or IP address of the managed system that triggered the event.
Object Name	The name of the selected entitlement.
Event	The type of operation made to the selected entitlement: • Create • Delete • Update • Add Membership • Remove Membership NOTE: A membership operation indicates a relationship change with a related or parent object such as a user or user group was added or removed from the membership of an entitlement.
Related Object	The name of the related object.
Related Object Type	The type of the related object.
Parent	The name of the object to which the selected entitlement is a child.
Parent Object Type	The parent object type.

Managing entitlements

Use the controls and tabbed pages on the **Entitlements** page to perform the following tasks to manage SPP entitlements:

- Adding an entitlement
- Adding users or user groups to an entitlement
- Creating an access request policy
- Deleting an access request policy
- Copying an access request policy
- Deleting an entitlement

Adding an entitlement

It is the responsibility of the Security Policy Administrator to add entitlements to SPP.

To add an entitlement

1. Navigate to **Security Policy Management** > **Entitlements**.
2. Click **+ New Entitlement** from the toolbar.
3. In the **New Entitlement** dialog, provide the following information on the General tab:
    - **Name**: Enter a unique name for the entitlement. Limit: 50 characters.
    - **Description**: Enter descriptive text about the entitlement. Limit: 255 characters.
    - **Priority**: Enter the priority of this entitlement compared to other entitlements.

      If a user desires to access an account in the scope of two different entitlements, then the entitlement with the highest priority (that is, the lowest number) takes precedence. For more information, see How SPP evaluates policy when a user submits an access request on page 505.
    - **Have the Entitlement Expire on Date and Time**: Select this option to enforce an expiration date, then enter the date and time.

      When an entitlement expires, all the access request policies associated with the entitlement also expire. To set an expiration date on a policy, see Creating an access request policy.

      > NOTE:
      >
      > An entitlement's time restrictions enforce when SPP uses a policy. A policy's time restrictions enforce when a user can access the account passwords. If the entitlement and the policy both have time restrictions, the user can only check out the password for the overlapping time frame.

> Time restrictions control when the entitlement or policy is in effect relative to a user's time zone. Although SPP Appliances run on Coordinated Universal Time (UTC), the user's time zone enforces the time restrictions set in the entitlement or policy. This means that if the appliance and the user are in different time zones, SPP enforces the policy in the user's time zone set in their account profile.
>
> User can change their time zone, by default. Or, the User Administrator can prohibit a user from changing the time zone, possibly to ensure adherence to policy. For more information, see Time Zone.Time Zone in the *Safeguard for Privileged Passwords Administration Guide*.

- **Use Time Windows**: Select this option to enforce time windows.

  Select and drag to highlight the hours you want to allow. Colored tiles are blocked times. Clear are available times.

4. Select one of the following save options:
   - **Save & Close**: This option saves the entitlement then returns you to the **Entitlements** page.
   - **Save & Continue**: This option saves the entitlement then sends you to the Access Request Policies tab (entitlements) for further configuration options. These settings are also available when selecting to edit an entitlement.

Related Topics

How SPP evaluates policy when a user submits an access request

Adding users or user groups to an entitlement

How SPP evaluates policy when a user submits an access request

An entitlement defines which users are authorized to check out passwords for accounts in the scope of the account's policies. A policy defines scope (that is, which accounts) and the rules for checking out passwords, such as the duration, how many approvals are required, and so on.

It is possible for an account to be governed by more than one entitlement, or is in the scope of more than one policy within an entitlement. When evaluating which policy governs a request to grant access, SPP first determines if the request has Emergency Access and evaluates against only those policies which permit Emergency Access. It then considers the time for which the request is being made and further evaluates against only those policies which have Time Restrictions that permit the request. Finally, if there is a conflict between the remaining policies, it uses Priority to determine which policy should govern the request.

Example scenario:

- Entitlement A (priority 1)
  - Policy: Week Day Policy.
    - Policy time restrictions: Monday through Friday 08:00 to 17:00.
    - Scope: AccountX
- Entitlement B (priority 2)
  - Policy 1: Sunday AM (priority 1)
    - Policy time restrictions: Sunday 08:00 to 12:00.
    - Scope: AccountX
  - Policy 2: Sunday PM (priority 2)
    - Policy time restrictions: Sunday 13:00 to 17:00.
    - Scope: AccountX

Notice that AccountX is in the scope of all three of these policies.

If a user requests the password for AccountX for Sunday at 16:00, SPP first considers Entitlement A because it is priority 1. When it determines that the policy time restrictions prevent the password release, it then considers Entitlement B.

SPP first considers Entitlement B's priority 1 policy. When it determines that the time restrictions prevent the password release, it then considers Policy 2. Once the request is satisfied, SPP grants the request.

However, if the hours in Entitlement B's Policy 1 were instead 08:00 to 17:00 then Policy 1 would be preferred because it has a higher priority. And if Entitlement B's Policy 2 was instead configured to allow Emergency Access, and the request being made had Emergency Access, then Policy 1 (though it has a higher priority of 1) would be eliminated from the selection and Policy 2 would again be preferred.

Creating an access request policy

It is the responsibility of the Security Policy Administrator to define access request policies in SPP.

A policy defines:

- The scope, which may be assets, asset groups, accounts, or account groups.
- The access type, which may be a:
  - Credential access type:
    - Password Release
    - SSH Key
    - API Key
  - Session access type:

    - RDP (Remote Desktop Protocol)
    - RDP Application
    - SSH (Secure SHell)
    - Telnet
- The rules for checking out passwords, such as the duration, how many approvals are required, and so on.

Considerations

- An access request policy is only assigned to one cluster.
- An access request policy is only used in the entitlement in which it is created. If you delete an entitlement, all access request policies associated with that entitlement are deleted.

To add an access request policy to an entitlement

1. Navigate to **Entitlements**.
2. In **Entitlements**, select to edit an entitlement from the list and open the **Access Request Policies** tab.
3. Click **+ New Access Policy** from the details toolbar.
4. In the **Create Access Request Policy** dialog, provide information in each of the tabs:

General tab (create access request policy)	Where you add general information about the access request policy as well as specify the type of access being requested.
Security tab (create access request policy)	Where you define the access settings for the selected type of request including allowing users to request passwords from their respective linked accounts.
Scope tab (create access request policy)	Where you assign assets, asset groups, accounts, or account groups to an access request policy.
Workflow tab (create access request policy)	Where you configure the access request policy requester, approver, reviewer settings.

General tab (create access request policy)

On the General tab, enter the following information for the access request policy.

Navigate to:

- web client: **Security Policy Management** > **Entitlements** > **Access Request Policies** > (create or edit a policy)

Table 207: Access Request Policy: General tab properties

Property	Description
Name	Enter a unique name for the access request policy. Limit: 50 characters
Description	Enter descriptive text that explains the access request policy. Limit: 255 characters
Priority	The priority of this policy compared to other policies in this entitlement. If a user desires to access an account in the scope of two different request polices within an entitlement, then the policy with the highest priority (that is, the lowest number) takes precedence. For more information, see How SPP evaluates policy when a user submits an access request on page 505.

Choose Request Policy Type	Specify the type of request policy:
	• Credential
	  • Password
	  • SSH Key
	  • API Key
	• Session
	  • RDP (Remote Desktop Protocol)
	  • RDP Application
	  • SSH (Secure SHell)
	  • Telnet

Choose Credential Type	Specify the type of credential: • Password • SSH Key • API Key NOTE: You can configure an access request policy for a password, SSH key, or API key request; however, if the Privileged Passwords module license is not installed, you will not be able to submit a password, SSH key, or API key release request. Similarly, you can configure an access request policy for a session request; however, if the Safeguard for Privileged

Property	Description
	Sessions server is not joined to SPP, you will be unable to submit a session request. NOTE: When checking out API keys, since multiple API keys may be associated with an account it will check out all the API Keys.
Have the Access Policy Expire on Date and Time	Select this to enforce an expiration date for the policy. Enter the expiration date and time.
Use Time Windows	Select this option to enforce time windows. Select and drag to highlight the hours you want to allow. Colored tiles are blocked times . Clear are available times.

Security tab (create access request policy)

Use the **Access Config** tab to configure the access settings for the type of access being requested, based on the access type specified on the General tab.

Navigate to:

- web client: **Security Policy Management** > **Entitlements** > **Access Request Policies** > (create or edit a policy)

Table 208: Access Request Policy: Access Config tab properties

Property	Description
Include password release with sessions requests	If **Access Type** is RDP, SSH, or Telnet, select this check box to include a password release with session access requests.
Include SSH Key release with sessions requests	If **Access Type** is RDP, SSH, or Telnet, select this check box to include an SSH Key release with session access requests.
Close expired sessions	If **Access Type** is RDP, SSH, or Telnet, select this check box to close sessions that have expired.
Change password after check-in	Select this check box if the password is to be changed after the user checks it back in. This check box is selected by default.
Change SSH key after check-in	Select this check box if the SSH key is to be changed after the user checks it back in. This check box is selected by default.

Property	Description
Passphrase Protect SSH Key	If **Access Type** is SSH Key, select this check box to require a passphrase for the SSH key.
Allow simultaneous access	Select this check box to allow multiple users access to the accounts and assets governed by this policy. Use the next check box to identify how many users can have access at once.
Maximum users at one time	When the **Allow simultaneous access** option is selected, enter the maximum number of users that can request access at one time.

Asset-Based Session Access	If **Access Type** is RDP, RDP Application, SSH, or Telnet, select one of the following options to define the type of account credentials to be used to access any of the assets defined in the policy scope, in addition to the accounts defined in the policy scope when a session is requested:
	• None: (Default) The credentials are retrieved from the vault when the session is requested.
	• User Supplied: (Only RDP, SSH, or Telnet) The requester user must provide the credentials when the session is requested.
	• Linked Account: The requester user's account is linked to a directory account that will be used when the session is requested.
	  • Enable scope filtering for linked accounts: When selected, this setting allows you to limit the number of requestable accounts to linked accounts that are also defined in the policy scope.
	  NOTE: If the policy scope includes only assets/asset groups and no accounts, then the scope filtering setting has no effect, and the policy is available to all of the linked directory accounts on each scoped policy asset.
	• Directory Account: Use the **Browse** button to select one or more directory accounts to be used when the session is requested.
	  If the Directory Account was migrated from an SPP version prior to 2.7, the directory account identifier may be blank, because earlier SPP versions understood only one assignment and version 2.7 results in multiple assignments.

Allow password access to linked accounts	If **Access Type** is Password Release, select this check box to allow users to request passwords for their respective linked account. Access to each user's linked account is governed by the other configurations defined in this policy. Additionally, **Enable scope filtering for linked accounts** can be selected in order to limit the number of requestable accounts to linked accounts that are also defined in the scope.

Property	Description
SPS Connection Policy	Use this drop-down to select a Safeguard for Privileged Sessions connection policy to use with the access request policy.
RDP Host Asset	If **Access Type** is RDP Application, use the **Browse** button associated with this field to select the asset configured to connect with the Windows Application Server.
Require Host Account	If **Access Type** is RDP Application, select this checkbox and then click **Browse** to locate the host account to use. When deselected, you will be prompted for the information when the session is initialized.
Application Display Name	If **Access Type** is RDP Application, this is the display name for the application that was provided when the remote application was published on the Windows application server.
Use Application Alias	If **Access Type** is RDP Application, this is the alias name defined when the remote application was published on the Windows application server. Ensure the full alias path is used, including the two vertical bars before the alias name (for example, ||OISGRemoteAppLauncher). If this option is used, the **Use Application Path and Command Line** option will not be available.
Use Application Path and Command Line	If **Access Type** is RDP Application, this option contains the following 2 fields: • **Application Path (path to the remove application)**: Enter the full path of an application program relative to the Windows host it will be running on. • **Application Command Line (parameters for the remote application)**: The Application Command Line contains the command line parameters to the application specified in the Application Path. The command line depends on the application. For example, some applications may require a set command line that will include the full path of the remote application along with its command line parameters while other applications may not require a set command line at all. If this option is used, the **Use Application Alias** field will not be available.
Use Alternate Login Name	If this option is selected, the alternate login name for the account will be used.

Scope tab (create access request policy)

Use the **Scope** tab in the web client to assign accounts, account groups, assets, and asset groups to an access request policy.

To assign accounts, account groups, assets, and asset groups to an access request policy

1. In the web client, navigate to **Security Policy Management** > **Entitlements** > **Access Request Policies**, then create or edit a policy.
2. On the **Scope** tab:
   a. Click **+ Add** from the details toolbar and select one of the following options:
      - **Add accounts to this policy**
      - **Add account groups to this policy**
      - **Add an asset to this policy**
      - **Add an asset group to this policy**
   b. In the dialog, make a selection, and click **OK**.

      If you do not see the selection you are looking for, depending on your Administrator permissions, you can create it in the dialog. (You must have Asset Administrator permissions to create accounts and assets. You must have Security Policy Administrator permissions to create account groups and asset groups.)
3. Repeat step one to make additional selections. You can add multiple types of objects to a policy; however, you can only add one type of object, like an accounts or account group, at a time.

All of the selected objects appear on the **Scope** tab in the **Access Request Policy** dialog. To remove an object from the list, select the object and click **− Delete**.

Workflow tab (create access request policy)

In the web client, the **Workflow** tab is split in to three tabs that allow you to configure the requester, approver, and reviewer settings for an access request policy:

Navigate to:

- web client: **Security Policy Management** > **Entitlements** > **Access Request Policies** > (create or edit a policy)

Requester tab

Use the **Requester** tab to specify the requester settings for an access request policy.

Table 209: Access Request Policy: Requester tab properties

Property	Description
Duration of Access Approval	Enter or select the default duration (days, hours, and minutes) that the requester can access the accounts and assets governed by this policy. The access duration cannot exceed a total of 31

Property	Description
	days (44,640 minutes).
Allow Requester to Change Duration	Select this check box to allow the requester the ability to modify the access duration.
Maximum Time Requester Can Have Access	If you select the **Allow Requester to Change Duration** option, you can set the maximum duration (days, hours, and minutes) that the requester can access the accounts and assets governed by this policy. The default access duration is seven days. The maximum access duration is 31 days. The users can change the access duration, but they cannot access the accounts or assets governed by this policy for longer than the maximum access duration time.
Allow Emergency Access	Select this option to allow users to request emergency access to accounts and assets governed by this policy. Clear this option to disallow emergency access. **Emergency Access** overrides the **Approver** requirements; that is, when a user requests access using **Emergency Access**, the request is immediately approved, provided that the other constraints are met, such as the **Requester** settings. Multiple users are allowed to request emergency access simultaneously for the same account or asset.
Ignore Time Restrictions	Select this option to ignore time restrictions when a user requests emergency access. Clear this option if you want to enforce the time restrictions set for this policy and only allow emergency access during the specified time period.
Notify When Account is Released with Emergency access | To	(Optional) When emergency access is enabled, build an escalation notification contact list, by entering an email address or selecting **To** to choose an email address of a SPP user. You can enter email addresses for non-SPP users. To send event notifications to a user, you must configure SPP to send alerts. For more information, see Configuring alerts on page 95. IMPORTANT: SPP does not dynamically maintain the email addresses for an escalation notification contact list. If you change a SPP user's email address or delete a SPP user after creating a policy, you must update the email addresses in an escalation notification contact list manually. For more information, see User not notified on page 657.
Require Comment	Select this check box to require that a requester provide a **Comment** when making an access request.

Property	Description
Reasons	Click **+Add** to add one or more reasons to the selected access request policy. Then, when requesting access to a password, SSH key, or a session, a user can select a predefined reason from a list. Click **OK** to add a reason. NOTE: You must have reasons configured in SPP to use this option. For more information, see Reasons on page 534.. If you do not see the reason you are looking for, you can create a reason from the **Reasons** dialog by clicking the **+New** toolbar button.
Require Reason Code	Select this option to require that a requester provide a **Reason** when requesting access. This option is only available if you have selected **Reasons** for the policy. If you add reasons to a policy, and leave this option cleared, the users will have the option of choosing a reason; but they will not be required to select a reason.

Approver tab

Use the **Approver** tab to specify the approver settings for an access request policy.

Table 210: Access Request Policy: Approver tab properties

Property	Description
Auto-Approved	Select this option to automatically approve all access requests for accounts and assets governed by this policy.
Notify when Account is Auto-Approved | **To**	(Optional) When no approvals are required, enter an email address or select **To** to choose a user to notify when access is auto-approved. If you used the **To** button to add SPP users, you can use the ⊗ **Clear** icon to remove an individual address from this list. NOTE: To send event notifications to a user, you must configure SPP to send alerts. For more information, see Configuring alerts on page 95.
Approvals Required	Select this option to require approval for all access requests for accounts and assets governed by this policy. Enter the following information: • **Qty**: Enter or select the minimum number of approvals required from the selected users or user groups listed as **Approvers**. • **Approvers**: **Browse** to select one or more users or user groups who can approve access requests for accounts and

Property	Description
	assets governed by this policy. Click **+ Add an Approval Group** or **− Delete** to add or remove approver sets. The order of the approver sets is not significant, but all requirements must be met; that is, a request must obtain the number of approvals from each approver set defined. The users you authorize as approvers receive alerts when an access request requires their approval if they have SPP configured to send alerts. TIP: As a best practice, add user groups as approvers rather than individuals. This makes it possible to add an individual approver to a pending access request. In addition, you can modify an approvers list without editing the policy.
Notify if approvers have pending requests after **To**	(Optional) Select this check box to enable notifications. • Set the amount of time (days, hours, and minutes) to wait before notifying the escalation notification contact list about pending approvals. • Enter an email address or select **To** to choose an email address of a SPP user. You can enter email addresses for non-SPP users. IMPORTANT: SPP does not dynamically maintain the email addresses for an escalation notification contact list. If you change a SPP user's email address or delete a SPP user after creating a policy, you must update the email addresses in an escalation notification contact list manually. For more information, see User not notified on page 657. NOTE: To send event notifications to a user, you must configure SPP to send alerts. For more information, see Configuring alerts on page 95.
Cloud Assistant has been enabled. View enabled users.	Indicates that SPP is joined to Starling and registered as a sender with Cloud Assistant. Click the **users** link to view a list of the users who are authorized to approve requests using this feature. You can add users as Cloud Assistant approvers by clicking the **+ Add** toolbar button in the **Cloud Assistant Users** dialog.

Reviewer tab

Use the **Reviewer** tab to specify the reviewer settings for an access request policy.

Table 211: Access Request Policy: Reviewer tab properties

Property	Description
Review Not Required	This check box is selected by default, indicating that no review is required for completed access requests for accounts and assets governed by this policy.
Review Required	Select this check box to require a review of completed access requests for accounts and assets governed by this policy. • **Qty**: Enter or select the minimum number of people required to review a completed access request. • **Browse** to select one or more users or groups of users who can review access requests for accounts and assets governed by this policy. A reviewer can only review an access request once it is completed. The users you authorize as reviewers receive alerts when an access request requires their review if they have SPP configured to send alerts. TIP: As a best practice, add user groups as reviews rather than individuals. This makes it possible to add an individual reviewer to a pending access request. In addition, you can modify a reviewers list without editing the policy.
Require Comment	Select this check box if the reviewer is required to enter a comment when reviewing an access request.
Pending Reviews Do Not Block Access	Select this check box when you want to allow new access requests whether a prior request is approved or not approved. In other words, no requests will be blocked based on the approval status of a prior request.
Notify If Reviewers Have Pending Reviews After **To**	(Optional) Select this check box to enable notifications. • Set the amount of time (days, hours, and minutes) to wait before reminding the escalation notification contact list about pending reviews. • Enter an email address or select **To** to choose an email address of a SPP user. You can enter email addresses for non-SPP users. To send event notifications to a user, you must configure SPP to send alerts. For more information, see Configuring alerts on page 95. IMPORTANT: SPP does not dynamically maintain the email addresses for an escalation notification contact list. If you change a SPP user's email address or delete a SPP user after

Property	Description
	creating a policy, you must update the email addresses in an escalation notification contact list manually. For more information, see User not notified on page 657.

Adding users or user groups to an entitlement

When you add users to an entitlement, you are specifying which people can request passwords to the accounts governed by the selected entitlement's access request policies, or which people can request sessions for the accounts and assets governed by the selected entitlement's access request policies. A user can be a Sessions Appliance certificate user. For more information, see Session Appliances with Safeguard for Privileged Sessions link on page 208.

It is the responsibility of the Security Policy Administrator to add users to entitlements. The Security Policy Administrator only has permission to add groups, not users. For more information, see Administrator permissions on page 604.

To add requester users to an entitlement

1. Navigate to **Security Policy Management** > **Entitlements**.
2. In **Entitlements**, select an entitlement from the list and click the **Users** tab.
3. Click **+ Add Users** or **Add User Groups** from the details toolbar.
4. Select one or more users or user groups from the list in the **Users** or **User Groups** dialog.
5. Click **OK**.

Deleting an access request policy

IMPORTANT: When you delete a policy, SPP deletes it permanently, but it does not delete the accounts governed by the policy.

To delete an access request policy from an entitlement

1. Navigate to **Security Policy Management** > **Entitlements**.
2. In **Entitlements**, select an entitlement from the list and open the **Access Request Policies** tab.
3. Select a policy.
4. Click **Delete**.
5. Confirm your request.

Modifying an access request policy

Access request polices can be migrated. For more information, see Creating an access request policy.

To modify an access request policy

1. Navigate to **Security Policy Management** > **Entitlements**.
2. In **Entitlements**, select an entitlement and open the **Access Request Policies** tab.
3. Double-click a policy, or select a policy and click **Edit**.
4. Select the tab of the policy's information you want to modify.

Copying an access request policy

You cannot copy a policy and add it to another entitlement; policies are entitlement-specific.

To copy an access request policy

1. Navigate to **Security Policy Management** > **Entitlements**.
2. In **Entitlements**, select an entitlement from the list and open the **Access Request Policies** tab.
3. Choose a policy and click **Create a New Access Policy from the Selected Row**.
4. Edit the new policy's settings as desired.

Deleting an entitlement

IMPORTANT: When you delete an entitlement, SPP deletes all access request policies associated with that entitlement.

To delete an entitlement

1. Navigate to **Security Policy Management** > **Entitlements**.
2. In **Entitlements**, select an entitlement from the list.
3. Click **Delete**.
4. Type the word `delete` to confirm you want to delete the entitlement.
5. Click **Yes**.

Linked Accounts

Within the web client, the **Linked Accounts** page displays information on the directory accounts and the users associated with them.

To access **Linked Accounts**:

- web client: Navigate to **Security Policy Management** > **Linked Accounts**.

The **Linked Accounts** page is separated into two tabs:

- Users (linked accounts)
- Accounts (linked accounts): This page lists the linked accounts.

Users (linked accounts)

Within the web client, the **Users** tab on the **Linked Accounts** page displays information on the users associated with linked accounts.

To access the **Users** tab on the **Linked Accounts** page:

- web client: Navigate to **Security Policy Management** > **Linked Accounts** which by default displays the **Users** tab.

Toolbar

Use these toolbar buttons to manage users:

- **Edit**: Select a user then click this button to open additional information and options; including linking an account to the user.
- **Refresh**: Update the list of users.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Accounts (linked accounts)

Within the web client, the **Accounts** tab on the **Linked Accounts** page displays information on the accounts currently linked to users.

To access the **Accounts** tab on the **Linked Accounts** page:

- web client: Navigate to **Security Policy Management** > **Linked Accounts** and open the **Accounts** tab.

Toolbar

Use these toolbar buttons to manage accounts:

- **Edit**: Select an account then click this button to open additional information and options; including linking a user to an account.
- **Refresh**: Update the list of accounts.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Managing linked accounts

Use the controls and tabbed pages on the **Linked Accounts** page to perform the following tasks to manage linked accounts:

- Linking a user to an account
- Linking an account to a user
- Removing a linked account from a user
- Removing a user from a linked account

Linking a user to an account

It is the responsibility of the Security Policy Administrator to link a user to an account. Once linked, these linked accounts can be used to access assets and accounts within the scope of an access request policy.

To link a user to an account

1. Navigate to **Security Policy Management** > **Linked Accounts**.
2. On the **Users** tab, select a user from the object list and click **Edit**.
3. Click **+ Add** from the details toolbar.

   The **Select Directory Account** dialog displays, listing the directory accounts available in SPP.
4. Select one or more accounts from the list in the **Select Directory Account** dialog and click **OK**.

Linking an account to a user

It is the responsibility of the Security Policy Administrator to link an account to a user. Once linked, these linked accounts can be used to access assets and accounts within the scope of an access request policy.

To link an account to a user

1. Navigate to **Security Policy Management** > **Linked Accounts**.
2. On the **Accounts** tab, select an account from the object list and click **Edit**.
3. Click **+ Add** from the details toolbar.

   The **Users** dialog displays, listing the users available in SPP.
4. Select one or more users from the list in the **Users** dialog and click **OK**.

Removing a linked account from a user

It is the responsibility of the Security Policy Administrator to remove linked accounts from a user.

To remove a linked account from a user

1. Navigate to **Security Policy Management** > **Linked Accounts**.
2. On the **Users** tab, select a user from the object list and click **Edit**.
3. Select a linked account (or accounts) from the list.
4. Click **Remove** from the details toolbar.
5. A confirmation dialog will appear confirming the account(s) being removed. Click **Yes**.

Removing a user from a linked account

It is the responsibility of the Security Policy Administrator to remove a user from a linked account

To remove a user from a linked account

1. Navigate to **Security Policy Management** > **Linked Accounts**.
2. On the **Accounts** tab, select an account from the object list and click **Edit**.
3. Select a user (or users) from the list.

4. Click **Remove** from the details toolbar.
5. A confirmation dialog will appear confirming the user(s) being removed. Click **Yes**.

User Groups

NOTE: The User Groups page is accessible from the following locations:

- **Security Policy Management** > **User Groups**
- **User Management** > **User Groups**

SPP allows you to either create a local group that exists and is managed within SPP only, or add a directory group that is synchronized from an external Active Directory or LDAP server. Then a Security Policy Administrator can add one or more user groups to an entitlement, which will authorize members of the group(s) to request access to the accounts and assets governed by the entitlement's access request policies.

User Groups is available to the Authorizer Administrator, User Administrator, Security Policy Administrator, Help Desk Administrator, Auditor, and Asset Administrator. Not all functionalities will be available to all user types.

The User Groups view displays the following information about the selected user or directory group.

- Properties tab (user groups): Displays general information about the selected user group.
- Users tab (user groups): Displays the members of the selected group.
- Entitlements tab (user groups): Displays the entitlements for which the group has been assigned to. All members of the group then inherit access to the request policies of the entitlement.

  NOTE: The **Entitlements** tile is only visible to the Auditor and Security Policy Administrator.
- History (user): Displays the details of each operation that has affected the selected group.

Use these toolbar buttons to manage users.

- **User Group**: Add user groups to SPP. For more information, see Adding a user group on page 555.
- **Directory User Group**: Add a directory user group to SPP. For more information, see Adding a directory user group on page 556.
- **SCIM User Group**: Add SCIM user groups to SPP. For more information, see Adding a SCIM user group.

- **Delete**: Remove the selected user group. For more information, see Deleting a user group on page 561.
- **Edit**: Edit the selected user group.
- **Synchronize Now**: After selecting a user group from the table, use this button to manually prompt the synchronization process.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of user groups.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Properties tab (user groups)

The **Properties** tab lists information about the selected user group.

To access **Properties**:

- web client: Navigate to **Security Policy Management** > **User Groups** > (New) or (Edit) > **Properties** or **User Management** > **User Groups** > **Properties**.

Table 212: User Groups: Properties tab properties

Property	Description
Name	The entitlement name.
Description	Information about the selected entitlement.
Delete	Click this button to delete the user group.

The **Properties** > **Permissions** tab lists the user's administrator permissions or "Standard User" if the user does not have administrative permissions.

Users tab (user groups)

The **Users** tab displays the members of the selected group.

Click **+ Add User** from the details toolbar to add one or more users to the selected local user group.

NOTE: For directory groups, group membership is read-only. That is, you cannot add or remove users from a directory group using the **Users** tab.

To access **Users**:

- web client: Navigate to **Security Policy Management** > **User Groups** > (Edit) > **Users** or **User Management** > **User Groups** > (Edit) > **Users**.

Table 213: User Groups: Users tab properties

Property	Description
Username	The user's display name.
Name	The user's first and last name, if the information exists in the user's properties; otherwise, the user's display name.
Description	Description of the user.
Provider	The name of the authentication provider: **Local**, **Certificate**, or the name of an external provider such as a Microsoft Active Directory domain name.
Distinguished Name	The distinguished name of the user.
Last Name	The user's last name.
First Name	The user's first name.
Email	The user's email address.
Work Phone	The user's work phone.
Mobile Phone	The user's mobile phone.
Time Zone	The user's time zone.
Identity Provider	The user's identity provider.
Domain Name	The domain name for the user.
Login Name	The user's login name.
Deactivated	This column indicates if a user is currently deactivated.
Permissions	The user's permissions.

Use these buttons on the details toolbar to manage the users in your user groups.

Table 214: User Groups: Users tab toolbar

Option	Description
Add User	Add one or more users to the selected user group. For more information, see Adding users to a user group on page 560.

Option	Description
Remove	Remove the selected user from the user group.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of users in the user groups.
Search	To locate a specific user or set of users in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Entitlements tab (user groups)

The **Entitlements** tab displays the entitlements for which the group has been assigned to. All members of the group then inherit access to the request policies of the entitlement.

NOTE: The **Entitlements** tab is only available to a user with Auditor or Security Policy Administrator permissions.

Click **+Add Entitlement** to add the selected user group as a user of one or more entitlements.

To access **Entitlements**:

- web client: Navigate to **Security Policy Management** > **User Groups** > (Edit) > **Entitlements** or **User Management** > **User Groups** > (Edit) > **Entitlements**.

Table 215: User Groups: Entitlements tab properties

Property	Description
Name	The name assigned to the entitlement.
Accounts	The number of unique accounts in this entitlement.
Users	The number of unique users and user groups in this entitlement.
Policies	The number of unique policies in this entitlement.

Use these buttons on the details toolbar to manage the entitlements associated with the selected user group.

Table 216: User Groups: Entitlements tab toolbar

Option	Description
Add	Add the selected user group to one or more entitlements. For more information, see Adding a user group to an entitlement on page 561.
Remove	Remove the user group from the selected entitlement.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of entitlements.
Search	To locate a specific entitlement or set of entitlements in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

History tab (user groups)

The **History** tab allows you to view or export the details of each operation that has affected the selected group.

To access **History**:

- web client: Navigate to **Security Policy Management** > **User Groups** > (Edit) > **History** or **User Management** > **User Groups** > (Edit) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
  - **Refresh**: Update the list displayed.
  - **Search**: For more information, see Search box on page 78.

Table 217: User Groups: History tab properties

Property	Description
Date/Time	The date and time of the event
User	The display name of the user that triggered the event
Source IP	The network DNS name or IP address of the managed system that

Property	Description
	triggered the event
Object Name	The name of the selected group
Event	The type of operation made to the selected user group: • Create • Delete • Update • Add Membership • Remove Membership • Directory Group Sync Complete NOTE: A membership operation indicates a relationship change with a related or parent object such as a user was added or removed from the membership of the selected user group or the selected group was added or removed from an entitlement.
Related Object	The name of the related object
Related Object Type	The type of the related object
Parent	The name of the object to which the selected user group is a child
Parent Object Type	The parent object type

Managing user groups

Use the controls and tabbed pages on the User Groups page to perform the following tasks to manage SPP user groups:

- Adding a user group
- Adding a directory user group
- Adding a SCIM user group
- Adding users to a user group
- Adding a user group to an entitlement
- Deleting a user group

Adding a user group

It is the responsibility of the Security Policy Administrator, Authorizer Administrator, and User Administrator to add groups of users to SPP.

To add a user group

1. Navigate to **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. Click **+ New User Group** from the toolbar and select **User Group**.
3. In the **New User Group** dialog, enter the following information:
   a. **Name**: Enter a unique name for the user group.

      Limit: 50 characters

   b. **Description**: (Optional) Enter information about this user group.

      Limit: 255 characters
4. On the **Permissions** tab, select **Help Desk** and/or the **Personal Password Vault** permission to be assigned to each member of the **Group**. For each group member, the selected permissions of the Group will be combined with any existing permissions that have already been granted explicitly or by some other Group to which they belong. For more information, see the Permissions tab (add user).
   During synchronization of a Group (which occurs every 15 minutes), a user may be identified as no longer being a member. In this case, the selected permissions of the Group are removed from the user unless the user is also a member of another Group from which they inherit the permission. SPP does not keep track of nor distinguish between an explicitly assigned permission versus one that was assigned via a Group.

   > IMPORTANT: The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Groups from which they inherited it, the user will no longer be able to access **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission again, they regain access to all of their existing data.
5. Click **OK**. On an import, the user group is created and the assigned users appear when the import process is complete.

Adding a directory user group

In order to add a directory user group, an Appliance Administrator must add an Active Directory or LDAP server as an identity provider.

- web client: Navigate to **Appliance Management** > **Safeguard Access** > **Identity and Authentication**.

  For more information, see Identity and Authentication on page 254.

Next, the Authorizer Administrator or the User Administrator can add directory user groups.

The Security Policy Administrator, Authorizer Administrator, and User Administrator can add local user groups. For more information, see Adding a user group on page 555.

Import consideration

All users who are part of a directory import user group must have complete and valid attributes. If the attributes for a user are not complete and valid, the user is not imported and the import continues.

Port

The standard global catalog port, 3268 (LDAP), must be open on the firewall for every Windows global catalog server in the environment and SPP Appliance to communicate for directory management tasks (for example, adding a directory account, a directory user account, or a directory user group). LDAP uses port 389 for unencrypted connections. For more information, see the Microsoft publication How the Global Catalog Works.

Time

Because Microsoft Active Directory does not have a Time Zone attribute, when you add a directory group, the default time zone is set for all imported accounts to (UTC) Coordinated Universal Time. To reset the time zone, open each imported account in **Users** and modify the Time Zone on the **Location** tab.

To add a directory user group

1. Navigate to **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. Click **+ New User Group** from the toolbar and select **Directory User Group**.
3. In the **Directory Group** tab:
   a. Select a directory.
   b. For **Filter Search Location**, use **Browse** to select a container within the directory. This option is not available for Starling directories.
   c. The **Include objects from sub containers** check box is selected by default indicating that child objects will be included in your search. Clear this check box to exclude child objects from your search. This option is not available for Starling directories.
   d. In the **Contains** field, enter a full or partial directory group name and click **Search**. Or leave blank to return the first 1,000 items.

      The text search is not case-sensitive and does not allow wild cards. SPP searches each domain of a forest. You can search on partial strings. For example, if you enter "ad" in the search box, it will find any directory group that contains "ad."
   e. Select a group name from the results displayed in the **Select the group to add** grid.
   f. At the bottom of the **Directory Group** dialog, select the **Automatically link Managed Directory Accounts** check box to have existing managed directory accounts set as linked accounts on the imported user. This option is not available for Starling directories.

Based on the setting of the identity provider's Managed Objects attribute, the attribute values are used to match up with existing managed directory accounts in Safeguard. The Safeguard user's set of linked accounts will periodically synchronize with the directory and be overwritten with the values from the directory. Any changes to the linked accounts made manually to the user are lost at the next directory synchronization (see **Sync additions every** under Management tab (add asset)).

4. In the **Authentication** tab, set the primary and secondary authentication. If you are importing users, Safeguard sets the primary and secondary authentication providers for new users. If a directory user group member already exists as a user in Safeguard, their authentication properties are not changed. To change authentication settings on existing Safeguard users that are members of the group, you must manually invoke the `/UserGroups/{id}/SynchronizeAndUpdateProviders` API method.
   Directory groups require the forest root domain to be visible and available for identity and authentication set on **Appliance Management** > **Safeguard Access** > **Identity and Authentication**. For more information, see Available Domains for Identity and Authentication (for Active Directory) on page 261.

   a. The **Authentication Provider** field defaults to the directory (or the forest root name for Active Directory) from which the group came.

      All newly created Safeguard users that are imported from the directory user group will have their primary authentication provider set to use the directory domain from which their user originates. For an Active Directory forest with multiple domains, the domains must be marked as **Available Domains for Identity and Authentication**. If a user is a member of a group, but their domain is not marked as **Available for Identity and Authentication**, the user will not be imported. For more information, see Adding identity and authentication providers on page 259.

      You can use either an External Federation or Radius server as each user's primary authentication provider. During an import process, the directory attribute that was specified for **External Federation Authentication** or **Radius Authentication** will be used to set the user's **Email Address** or **Name Claim** (for External Federation) or **Login name** (for Radius) property. See the External Federation settings attribute and Radius settings attribute for more information.

   b. Select the **Require Certificate Authentication** check box to require that the user logs in to Safeguard using their domain issued user certificate or SmartCard. This option is only available when the directory user group comes from Microsoft Active Directory and the **Authentication Provider** is also set as that directory.

   c. You can require the user to log in with two-factor authentication. Users being imported must have their contact information complete in order to successfully create a user in Safeguard.

      i. Select the **Require Secondary Authentication** check box. For more information, see Requiring secondary authentication log in on page 546.

ii. Choose the secondary **Authentication Provider** for all users of the directory user group. Use valid combinations of identity and authentication providers. For more information, see Identity and Authentication on page 254.

5. On the **Permissions** tab, select any of the administrative permissions and/or the **Personal Password Vault** permission to be assigned to each member of the **Directory Group**. For each group member, the selected permissions of the group will be combined with any existing permissions that have already been granted explicitly or by some other Group to which they belong. For more information, see the Permissions tab (add user).
   During synchronization of a Directory Group, a user may be identified as no longer being a member. In this case, the selected permissions of the Directory Group are removed from the user unless the user is also a member of another Group from which they inherit the permission. SPP does not keep track of nor distinguish between an explicitly assigned permission versus one that was assigned via a Group.

   > IMPORTANT: The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Groups from which they inherited it, the user will no longer be able to access **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission again, they regain access to all of their existing data.

6. Click **OK**. On an import, the directory user group is created and the assigned users appear when the import process is complete.
7. After adding the information, you can edit the following directory group settings and the directory synchronization process will be triggered in the background.
   - **Directory Group** tab: Select or clear the **Automatically link Managed Directory Accounts** check box.
   - **Authentication** tab: Change the authentication providers.

     > NOTE: Changing the authentication providers will only effect newly imported users. Existing users will not have their authentication providers updated. To change authentication settings on existing Safeguard users that are members of the group, you must manually invoke the `/UserGroups/{id}/SynchronizeAndUpdateProviders` API method.

   - **Permissions** tab: Change the permissions.

Adding users to a user group

It is the responsibility of an Authorizer Administrator, User Administrator, or Security Policy Administrator to add users to local SPP groups. For directory user groups, you cannot manually add or remove users. Instead, those groups will automatically be synchronized with the Active Directory or LDAP server they came from.

To add users to a user group

1. Navigate to:
   - web client: **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. In **User Groups**, select a user group from the object list and open the **Users** tab.
3. Click **+ Add User** from the details toolbar.
4. Select one or more users from the list in the **Users** dialog and click **OK**.

   IMPORTANT: You cannot add a group to a user group's membership; group membership cannot be nested.

Adding a user group to an entitlement

When you add user groups to an entitlement, you are specifying which people can request access to the accounts and assets governed by an entitlement's policies. It is the responsibility of the Security Policy Administrator to add user groups to entitlements.

To add a user group to entitlements

1. Navigate to:
   - web client: **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. In **User Groups**, select a user group from the object list and open the **Entitlements** tab.
3. Click **+ Add Entitlement** from the details toolbar.
4. Select one or more entitlements from the **Entitlements** dialog and click **OK**.

Deleting a user group

Both Authorizer Administrator and User Administrator can delete local and directory user groups. A Security Policy Administrator can only delete local groups without permissions on them.

When you delete a user group, SPP does not delete the users associated with it.

To delete a user group

1. Navigate to:
   - web client: **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. In **User Groups**, select a user group from the list.

3. Click 🗑 **Delete**.
4. Confirm your request.

Security Policy Settings

In the web client, **Security Policy Management** has a settings page used to manage Sessions Password Access and the Audit Log Stream Service. You can also manage the reasons for requesting access to a password, SSH key, or session.

Navigate to **Security Policy Management** > **Settings** to manage the settings listed below.

Table 218: Security Policy Settings

Setting	Description
Maximum Notification Recipients	Set the maximum number of notification recipients.
Expiration Warning Duration	Enter the number of days for the warning to expire.
Show User Name in Access Request Conflict Messages	When the check box is selected, if there is a conflicting access request for the time period a user wants to request, the error message will include the name of the user who requested the conflicting access request. When the check box is cleared, the error message will show the access request id instead. This check box is cleared by default.
Allow Access Request Search by Tags	This option allows you to find requestable accounts by searching for tags. This feature is disabled by default. NOTE: When the **Allow Access Request Search by Tags** option is turned off, the **Asset Tags** column, the **Account Tags** column, and the **Advanced Search** boxes are not available in the **New Access Request** window.
Session Password Access Enabled	Use this to enable or disable session password access. This feature is disabled by default.
Audit Log Stream Service	Use this to send SPP data to Safeguard for Privileged Sessions to audit the Safeguard privileged management software suite. The feature is disabled by default. To accept SPP data, the Safeguard for Privileged Sessions Appliance Administrator must turn on audit log syncing. For information, see the *Safeguard for Privileged Sessions Administration Guide*. SPP and Safeguard for Privileged Sessions must be linked to use

Setting	Description
	this feature. For more information, see SPP and Safeguard for Privileged Sessions appliance link guidance. While the synchronization of SPP and Safeguard for Privileged Sessions is ongoing, Safeguard for Privileged Sessions is not guaranteed to have all of the audit data at any given point due to some latency. NOTE: This setting is also available under **Appliance Management**. For more information, see Global Services.
Reasons	From this pane you can manage the reasons for requesting access to a password, SSH key, or session. For more information, see Reasons.

Reasons

In an access request policy, a Security Policy Administrator can require that a requester provide a reason for requesting access to a password, SSH key, or session. Then, when requesting access, the user can select a predefined reason from a list. For example, you might use these access request reasons:

- Software Updates
- System Maintenance
- Hardware Issues
- Problem Ticket

To configure access request reasons

1. Navigate to **Security Policy Management** > **Settings** > **Reasons**.
2. Click **+Add** to add a new reason.
3. In the **New Reason** dialog, enter the following:
   a. **Name**: Enter a name for the reason. Limit: 50 characters
   b. **Description**: Enter a description for the reason. Limit: 255 characters
4. Click **Save**.

To edit a reason, select a previously configured reason and click **Edit**.

To delete a reason, select a previously configured reason and click **Delete**.

13

User Management

In the web client, expand the **User Management** section in the left navigation pane.

Users

A user is a person who can log in to SPP. You can add both local users and directory users. Directory users are users from an external identity store such as Microsoft Active Directory. For more information, see Users and user groups on page 26. in *Overview of the Entities*.

Your administrator permissions determine what you can view in **Users**. Users displayed in a faded color are disabled. The following table shows you the tabs that are available to each type of administrator.

- Authorizer Administrator: General, History
- User Administrator: General, User Groups (directory users only), History
- Help Desk Administrator: General, History
- Auditor: General, Owned Objects, User Groups, Entitlements, Linked Accounts, History
- Asset Administrator: General, Owned Objects
- Security Policy Administrator: General, User Groups, Entitlements, Linked Accounts, History

The Authorizer Administrator typically controls the **Enabled/Disabled** state. For more information, see Activating or deactivating a user account on page 548.

Go to Users:

- web client: Navigate to **Security Policy Management** > **Users**

Users view

The **Users** view displays the following information about a selected user:

- Properties tab (user): Displays the authentication, contact information, location, and permissions for the selected user.
- User Groups tab (user): Displays the user groups in which the selected user is a member.
- Entitlements tab (user): Displays the entitlements in which the selected user is a member; that is, an entitlement "user".
- History (user): Displays the details of each operation that has affected the selected user.

Toolbar

Use these toolbar buttons to manage users:

- **+ New User**: Add users to SPP. For more information, see Adding a user on page 541.
- **Delete**: Remove the selected user. For more information, see Deleting a user on page 548.
- **View details**: View and edit the details for a selected user.
- **Permissions**: Display the **Permissions** dialog showing what administrative permissions apply to the selected user.
- **Set Password**: Use this option to set a password for a local user.
- **Unlock**: Use this option to unlock the account of a local user.
- **Activate User**: Use this option activate the account of a selected user.
- **Deactivate User**: Use this option to deactivate the account of a selected user.
- **Import**: Use this button to add users to One Identity Safeguard for Privileged Passwords using a CSV file. For more information, see Importing objects.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of users.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Properties tab (user)

The **Properties** tab lists information about the selected user.

To access **Properties** tab, in the web client, navigate to **User Management** > **Users** > **View Details** > **Properties**.

Table 219: Users Properties tab: Identity properties

Property	Description
Identity Provider	The source from which the user’s personal information comes from and is synchronized with.
Username	A user's display name.
First Name	The user's first name.
Last Name	The user's last name.
Work Phone	The user's work telephone number.
Mobile Phone	The user's mobile telephone number.
Email	The user's email address.
Description	The description text entered the user information was added or updated. This may be entered on the **User** dialog, **Identity** tab in the **Description** text box.
Location	User can change their time zone, by default. Or, the User Administrator can prohibit a user from changing the time zone, possibly to ensure adherence to policy. For more information, see Time Zone.Time Zone in the *Safeguard for Privileged Passwords Administration Guide*.

Table 220: Users Properties tab: Authentication properties

Property	Description
Authentication Provider	How the user authenticates with SPP: • **Certificate**: With a certificate • **Local**: With a user name and password. • **Directory name**: With directory credentials.
Login name	The identifier the user logs in with.
Domain Name	If the primary **Authentication Provider** is a directory, this indicates the directory's domain name.
Distinguished Name	The distinguished name for authentication.
Secondary Authentication	If you set up a user to require secondary authentication, this indicates the name of this user's secondary authentication service provider.
Secondary Authentication Username	The name of the user account on the secondary authentication service provider required at log in.
Password Never	When enabled, this field indicates the password associated with

Property	Description
Expires	the user does not expire.
User Must Change Password at Next Login	When enabled, this field indicates the user will be prompted to change their password the next time they login.
Require Certificate Authentication	When enabled, a certificate will be required for authentication.

Table 221: Users Properties tab: Permission properties

Property	Description
Permissions	Lists the user's administrator permissions or "Standard User" if user does not have administrative permissions.

User Groups tab (user)

The **User Groups** tab displays the user groups in which the selected user is a member.

The **User Groups** tab is available to a user with Auditor or Security Policy Administrator permissions and to the User Administrator for directory users (not for local users).

To access **User Groups**:

- web client: Navigate to **User Management** > **Users** > (View Details) > **User Groups**.

Use the following buttons on the details toolbar to manage the user groups associated with the selected user.

Table 222: Users: User Groups toolbar

Option	Description
Add	Add the user to one or more user groups to the user. For more information, see Adding a user to user groups on page 547.
Remove	Remove the selected user group from the selected user.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Retrieve and display an updated list of user groups associated with the selected user.
Search	To locate a specific user group in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Entitlements tab (user)

The **Entitlements** tab displays the entitlements in which the selected user is a member. The **Entitlements** tab is only available to a user with Auditor or Security Policy Administrator permissions.

To access **Entitlements**:

- web client: Navigate to **User Management** > **Users** > (View Details) > **Entitlements**.

Table 223: Users: Entitlements tab properties

Property	Description
Name	The name of the entitlements in which the selected user is assigned as a user.
Description	The description of the entitlement.
Policies	The number of unique access request policies in the entitlement.
Accounts	The number of unique accounts in the selected entitlement.
Users	The number of unique users in the entitlement.
User Groups	The names of the user groups that associate the selected user to the entitlement. NOTE: If the selected user is associated with the entitlement explicitly and not through user group membership, then this column is blank and the **Direct Member** column is **True**.
Direct Member	Indicates **True** if the selected user was explicitly added to the entitlement as a user. For more information, see Adding users or user groups to an entitlement on page 517.

Use the following buttons on the details toolbar to manage the entitlements associated with the selected user.

Table 224: Users: Entitlements tab toolbar

Option	Description
Add	Add the selected user as a user of one or more entitlements. For more information, see Adding a user to entitlements on page 547.
Remove	Remove the user from the selected entitlement.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.

Option	Description
Refresh	Update the list of entitlements.
Search	To locate a specific entitlement or set of entitlements in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

History (user)

On the **History** tab, administrators can view or **Export** the details of each operation that has affected the selected use on the **History** tab (except for Asset Administrators).

To access **History**:

- web client: Navigate to **User Management** > **Users** > (View Details) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
  - **Refresh**: Update the list displayed.
  - **Search**: For more information, see Search box on page 78.

Table 225: Users: History tab properties

Property	Description
Date/Time	The date and time of the event
User	The display name of the user that triggered the event
Source IP	The network DNS name or IP address of the managed system that triggered the event
Object Name	The name of the selected user.
Event	The type of operation made to the selected user: • Create • Delete • Update • Add Membership

Property	Description
	• Remove Membership NOTE: A membership operation indicates a "relationship" change with a related or parent object such as the selected user was added or removed from the membership of a user group or entitlement.
Related Object	The name of the related object.
Related Object Type	The type of the related object.
Parent	The name of the object to which the selected user is a child.
Parent Object Type	The parent object type.

Managing users

Use the controls and tabbed pages on the Users page to perform the following tasks to manage SPP users:

- Adding a user
- Requiring secondary authentication log in
- Adding a user to user groups
- Adding a user to entitlements
- Activating or deactivating a user account
- Deleting a user
- Setting a local user's password
- Unlocking a local user's account

Adding a user

It is the responsibility of either the Authorizer Administrator or the User Administrator to add SPP users.

To add a user

1. Navigate to **User Management** > **Users**.
2. In **Users**, click **+Add** from the toolbar.
3. In the **New User** dialog, provide information in each of the tabs:
    - Identity tab (add user): Where you define the identity provider, the user's contact information and location.

- Authentication tab (add user): Where you define the authentication provider, login name and password, if necessary.
- Permissions tab (add user): Where you set the user's administrator permissions.

Identity tab (add user)

On the **Identity** tab, choose an identity provider from the list of available providers. When adding a user from an external identity provider such as Microsoft Active Directory, SPP imports read-only contact information from the source, however, you can change the user photo.

Use valid combinations of identity and authentication providers. For more information, see Identity and Authentication on page 254.

Table 226: User: Identity tab properties

Property	Description
Identity Provider	The source of the user's identity. SPP comes with a built-in identity provider called **Local** that will allow you to manually enter user information that is stored directly in SPP. Or you can select an Active Directory or LDAP server that you have previously configured and then browse for a user. SPP will periodically synchronize with the directory to keep the information up to date. Indicate how the user's identity is managed by SPP: • Local • Active Directory • LDAP • Starling
Browse (Active Directory, Starling, or LDAP)	If the identity provider is Active Directory, Starling, or LDAP, click the **Browse** button to choose a username. The remaining fields are auto-populated.
Username (**Local** provider)	Enter the user's name that displays in the application. This is not the Login name which is set on the Authentication tab (add user).
First Name (**Local** provider)	Enter the user's first name. Limit: 30 characters; no double quotes.
Last Name (**Local** provider)	Enter the user's last name. Limit: 30 characters; no double quotes
Work Phone (**Local** provider)	Enter the user's work telephone number. Limit: 30 characters

Property	Description
Mobile Phone (**Local** provider)	Enter the user's mobile telephone number. Limit: 30 characters
Email (**Local** provider)	Enter the user's email address. Limit: 255 characters NOTE: Required for approvers using the Cloud Assistant feature and OneLogin MFA as their authentication provider. In addition, OneLogin MFA requires the email address entered in this field be identical to the email address configured in OneLogin.
Description (**Local** provider)	Enter information about this user. Limit: 255 characters.
Time Zone	Select the user's time zone. Because Microsoft Active Directory does not have a Time Zone attribute, when you add a directory group, the default time zone is set for all imported accounts to (UTC) Coordinated Universal Time. To reset the time zone, open each imported account in **Users** and modify the Time Zone on this **Location** tab.

Authentication tab (add user)

On the Authentication tab, specify the authentication settings for the user. An authentication provider can be the same or different as the user's identity provider.

Use valid combinations of identity and authentication providers. For more information, see Identity and Authentication on page 254.

Table 227: User: Authentication tab properties

Property	Description
Authentication Provider	Indicates how this user is to authenticate to SPP. The options are: • **Certificate**: With a certificate NOTE: SPP allows you to map a public-key certificate to a user account. You can then use the certificate to make authenticated requests to the appliance by means of the API. For more information, see Using the API on page 44. • **Local**: With a user name and password (default) • *<Directory name>*: With directory account credentials (only available if one or more directories have been added to SPP, such as Active Directory or LDAP, and the identity provider of the user is also that directory). • *<External Federation service provider name>*: With the

Property	Description
	credentials required by the External Federation or Radius server (only available if one or more of those authentication providers have been configured in SPP).
If Certificate provider: Certificate, Certificate Thumbprint (SHA-1)	If adding a **Certificate** user, enter the unique hash value (40 hexadecimal characters) of the certificate. You can copy and paste the Thumbprint value directly from the certificate, including the spaces.
If external federation provider: Email Address or Name Claim	If adding an external federation user account, enter the email address or name claim that will be returned from the STS of an authenticated user. A case-insensitive comparison will be performed on the value when the user is logging in. NOTE: You must configure or ensure that the STS includes either the email address claim or name claim. SPP will first look for the email address claim in the claims token. If that claim does not exist, it will use the name claim. You must create the user account in SPP according to what claim is returned by your STS, with precedence given to the email address claim.
If local or Radius as Primary provider: Login name	If using **Local** or **Radius as Primary** for authentication, this is the user's login name. This defaults to the value entered on the **Identity** tab, **Username** field. If using directory authentication, the login name is auto-populated.
Set Password button (editing an existing **Local** provider)	If you are editing an existing user for a **Local** provider, you may click **Set Password** to change a user's password. This button is not available when creating a new user or editing a user account from an external identity provider like Microsoft Active Directory.
Password (adding a **Local** provider)	If adding a **Local** user, enter a password for the user. You must comply with the password requirements specified in the dialog. For more information, see Local Password Rule on page 251.
Require Certificate Authentication (**Active Directory** provider if provider is MS AD)	Select this check box to require that the user logs into SPP using their domain issued user certificate or SmartCard. This option is only available when the **Authentication Provider** is a Microsoft Active Directory.
Password Never Expires	Select this check box to set a password that does not expire.
User must change	This check box is only available when using **Local** for authen-

Property	Description
password at next login	tication. When selected, this check box requires the user to change their password during their next login.
Require Secondary Authentication	Select this check box to require that this user logs in to SPP with two-factor authentication. For more information, see Requiring secondary authentication log in on page 546. Then choose the **Secondary Authentication Provider** for this user. Use valid combinations of identity and authentication providers. For more information, see Identity and Authentication on page 254.
Login Name (for secondary authentication; not used for FIDO2)	• When a directory is selected for secondary authentication, **Browse** to select the account on the secondary authentication provider this user must use when logging into SPP with two-factor authentication. • If Radius as a secondary authentication provider is selected, this value is pre-populated with the log in identifier. For more information, see Radius settings on page 266. A best practice is to have the users log in to validate the correct user is set up.

Permissions tab (add user)

On the Permissions tab, select the user's Administrator permissions, if applicable. For details on the rights for the permissions, see Administrator permissions.

Users permissions across multiple user groups

Users have permissions based on the user groups to which they are assigned. If a user is removed from a user group, the permissions related to that group are removed but the permissions for all other groups the user is assigned to remain in place.

User permissions on import

When a directory user group is imported, newly created Safeguard users are assigned the selected permissions. If the user exists in Safeguard, the selected permissions are added to the existing user permissions.For more information, see Adding a directory user group on page 556.

To assign permissions

When assigning permissions to a user, select the appropriate access controls. You can **Select all** or **Select none** at the bottom of the dialog.

- Authorizer: Allow the user to grant permissions to other users. This permission allows the user to change their own permissions.
- User: Allow the user to create new users, unlock and reset passwords for non-administrative users.
- Help Desk: Allow the user to unlock and set passwords for non-administrative users.
- Appliance: Allow the user to edit and update the appliance and to configure external integration settings, such as email, SNMP, Syslog, and Ticketing.
- Operations: Allow the user to reboot and monitor the appliance.
- Auditor: Allow the user read-only access encompassing all auditor roles. You can limit the Auditor role access by deselecting one of the following check boxes:
    - Application Auditor: Allow the user read-only access to Asset Management and Security Policy Management.
    - System Auditor: Allow the user read-only access to Appliance Management and User Management.
- Asset: Allow the user to add, edit, and delete partitions, assets, and accounts.
- Security Policy: Allow the user to add, edit, and delete entitlements and polices that control access to accounts and assets.
- Personal Passwords: Allow the user to add, edit, delete, share, and access the personal password vault. This check box is only available to the User Administrator and Security Policy Administrator. For more information, see Personal password vault on page 85.

Requiring secondary authentication log in

You can require a user to log in using two-factor authentication by enabling the **Require Secondary Authentication** option in the user record.

To require a user to log in using secondary authentication

1. Setup a secondary authentication provider in **Appliance Management** > **Safeguard Access** > **Identity and Authentication**. For more information, see Adding identity and authentication providers on page 259..
2. Configure the SPP user to **Require Secondary Authentication**. For more information, see Authentication tab (add user) on page 543..
    a. On the **Authentication** tab of a user's properties, select the **Require Secondary Authentication** check box.
    b. Choose the **Authentication Provider**.
    c. Depending on the type of authentication provider selected, specify the additional information this user must use when logging into SPP with two-factor authentication.
3. Log in with secondary authentication.

When you log in to SPP as a user which requires secondary authentication, you log in as usual, using the password that is set for the SPP user account. SPP then displays one or more additional login screens. Depending on how the system administrator has configured the secondary authentication provider, you must enter additional credentials for your secondary authentication service provider account, such as a secure password, security token code, or both.

> NOTE: The type and configuration of the secondary authentication provider (for example, RSA SecureID, FIDO2, and so on) determines what you must provide for secondary authentication. Check with your system administrator for more information about how to log in to SPP with secondary authentication.

Adding a user to user groups

It is the responsibility of the Security Policy Administrator to add users to user groups to assign to password policies.

To add a user to a user group

1. Navigate to **User Management** > **Users**.
2. In **Users**, select a user from the object list and open the **User Groups** tab.
3. Click **+Add** from the details toolbar.
4. Select one or more groups from the list in the**User Groups** dialog and click **OK**.

If you do not see the user group you are looking for and are a Security Policy Administrator, you can click **+ Create New** in the **User Groups** dialog and add the user group. For more information about creating user groups, see Adding a user group.

Adding a user to entitlements

It is the responsibility of the Security Policy Administrator to add users to entitlements. When you add users to an entitlement, you are specifying which people can request access governed by the entitlement's policies.

To add a user to entitlements

1. Navigate to **User Management** > **Users**.
2. In **Users**, select a user from the object list and open the **Entitlements** tab.
3. Click **+Add** from the details toolbar.
4. Select one or more entitlements from the list in the **Entitlements** dialog and click **OK**.

If you do not see the entitlement you are looking for and are a Security Policy Administrator, you can click **+Create New** in the **Entitlements** dialog. For more information about creating entitlements, see Adding an entitlement.

Activating or deactivating a user account

It is the responsibility of an Authorizer Administrator or User Administrator to activate or deactivate users within SPP. However, this state can only be changed within SPP on users that have their identity source set to the **Local** provider. This state cannot be modified for directory users. A directory user's state must be modified in the directory and then synchronized with SPP.

Deactivating a user will prevent that user from logging into SPP and end any currently logged in session. However, an administrator cannot deactivate their own user.

SPP can also be configured to automatically deactivate users who have not logged in within a configured time span. Note, this does not apply to directory users. For more information, see Local Login Control on page 247.

To activate or deactivate a user account

1. Navigate to **User Management** > **Users**.
2. In **Users**, select a user from the object list.
3. From the toolbar options, select either **Activate User** or **Deactivate User**.

Deleting a user

Typically, it is the responsibility of the Authorizer Administrator to delete administrator users and the User Administrator to delete non-administrator users.

> IMPORTANT: When you delete a local user, SPP deletes the user permanently. If you delete a directory user that is part of a directory user group, the next time it synchronizes its database with the directory, SPP will add it back in.

To delete a user

1. Navigate to **User Management** > **Users**.
2. In **Users**, select a user from the object list.
3. Click **Delete**.
4. Confirm your request.

Setting a local user's password

It is primarily the responsibility of the Authorizer Administrator to set passwords for administrators. The User Administrator and Help Desk Administrator set passwords for non-administrator local users. These administrators can only set passwords for local users. Directory user passwords are maintained in an external provider, such as Microsoft Active Directory.

To set a local user's password

1. Navigate to **User Management** > **Users**.
2. Select a local user from the object list and perform one of the following:
   - From the toolbar options, select **Set Password**.
   - On the **Properties** tab, click **Set Password**.
3. In the **Set Password** dialog, enter the new password.
4. If you want to require the user to change their password during their next login, make sure the **User must change password at next login** check box is selected.
5. Click **Set Password**. You must comply with the password requirements specified in the dialog. For more information, see Local Password Rule on page 251.

Unlocking a local user's account

If you are unable to log in, your account may have become "locked" and is therefore disabled. For example, if you enter a wrong password for the maximum number of times specified by the account **Lockout Threshold** settings, SPP locks your account. For more information, see Local Login Control on page 247.

Typically, it is the responsibility of the Authorizer Administrator to unlock administrator accounts, and the User Administrator and Help Desk Administrator to unlock non-administrator local users.

To unlock a local user's account

1. Navigate to **User Management** > **Users**.
2. Select a "locked" user from the list.
3. From the toolbar options, select **Unlock**.

User Groups

NOTE: The User Groups page is accessible from the following locations:

- **Security Policy Management** > **User Groups**
- **User Management** > **User Groups**

SPP allows you to either create a local group that exists and is managed within SPP only, or add a directory group that is synchronized from an external Active Directory or LDAP server. Then a Security Policy Administrator can add one or more user groups to an entitlement, which will authorize members of the group(s) to request access to the accounts and assets governed by the entitlement's access request policies.

User Groups is available to the Authorizer Administrator, User Administrator, Security Policy Administrator, Help Desk Administrator, Auditor, and Asset Administrator. Not all functionalities will be available to all user types.

The User Groups view displays the following information about the selected user or directory group.

- Properties tab (user groups): Displays general information about the selected user group.
- Users tab (user groups): Displays the members of the selected group.
- Entitlements tab (user groups): Displays the entitlements for which the group has been assigned to. All members of the group then inherit access to the request policies of the entitlement.

  NOTE: The **Entitlements** tile is only visible to the Auditor and Security Policy Administrator.
- History (user): Displays the details of each operation that has affected the selected group.

Use these toolbar buttons to manage users.

- **User Group**: Add user groups to SPP. For more information, see Adding a user group on page 555.
- **Directory User Group**: Add a directory user group to SPP. For more information, see Adding a directory user group on page 556.
- **SCIM User Group**: Add SCIM user groups to SPP. For more information, see Adding a SCIM user group.
- **Delete**: Remove the selected user group. For more information, see Deleting a user group on page 561.
- **Edit**: Edit the selected user group.
- **Synchronize Now**: After selecting a user group from the table, use this button to manually prompt the synchronization process.
- **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
- **Refresh**: Update the list of user groups.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Properties tab (user groups)

The **Properties** tab lists information about the selected user group.

To access **Properties**:

- web client: Navigate to **Security Policy Management** > **User Groups** > + (New) or (Edit) > **Properties** or **User Management** > **User Groups** > **Properties**.

Table 228: User Groups: Properties tab properties

Property	Description
Name	The entitlement name.
Description	Information about the selected entitlement.
Delete	Click this button to delete the user group.

The **Properties** > **Permissions** tab lists the user's administrator permissions or "Standard User" if the user does not have administrative permissions.

Users tab (user groups)

The **Users** tab displays the members of the selected group.

Click + **Add User** from the details toolbar to add one or more users to the selected local user group.

NOTE: For directory groups, group membership is read-only. That is, you cannot add or remove users from a directory group using the **Users** tab.

To access **Users**:

- web client: Navigate to **Security Policy Management** > **User Groups** > (Edit) > **Users** or **User Management** > **User Groups** > (Edit) > **Users**.

Table 229: User Groups: Users tab properties

Property	Description
Username	The user's display name.
Name	The user's first and last name, if the information exists in the user's properties; otherwise, the user's display name.
Description	Description of the user.

Property	Description
Provider	The name of the authentication provider: **Local**, **Certificate**, or the name of an external provider such as a Microsoft Active Directory domain name.
Distinguished Name	The distinguished name of the user.
Last Name	The user's last name.
First Name	The user's first name.
Email	The user's email address.
Work Phone	The user's work phone.
Mobile Phone	The user's mobile phone.
Time Zone	The user's time zone.
Identity Provider	The user's identity provider.
Domain Name	The domain name for the user.
Login Name	The user's login name.
Deactivated	This column indicates if a user is currently deactivated.
Permissions	The user's permissions.

Use these buttons on the details toolbar to manage the users in your user groups.

Table 230: User Groups: Users tab toolbar

Option	Description
Add User	Add one or more users to the selected user group. For more information, see Adding users to a user group on page 560.
Remove	Remove the selected user from the user group.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of users in the user groups.
Search	To locate a specific user or set of users in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

Entitlements tab (user groups)

The **Entitlements** tab displays the entitlements for which the group has been assigned to. All members of the group then inherit access to the request policies of the entitlement.

NOTE: The **Entitlements** tab is only available to a user with Auditor or Security Policy Administrator permissions.

Click **+Add Entitlement** to add the selected user group as a user of one or more entitlements.

To access **Entitlements**:

- web client: Navigate to **Security Policy Management** > **User Groups** > (Edit) > **Entitlements** or **User Management** > **User Groups** > (Edit) > **Entitlements**.

Table 231: User Groups: Entitlements tab properties

Property	Description
Name	The name assigned to the entitlement.
Accounts	The number of unique accounts in this entitlement.
Users	The number of unique users and user groups in this entitlement.
Policies	The number of unique policies in this entitlement.

Use these buttons on the details toolbar to manage the entitlements associated with the selected user group.

Table 232: User Groups: Entitlements tab toolbar

Option	Description
+Add	Add the selected user group to one or more entitlements. For more information, see Adding a user group to an entitlement on page 561.
−Remove	Remove the user group from the selected entitlement.
Export	Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
Refresh	Update the list of entitlements.
Search	To locate a specific entitlement or set of entitlements in this list, enter the character string to be used to search for a match. For more information, see Search box on page 78.

History tab (user groups)

The **History** tab allows you to view or export the details of each operation that has affected the selected group.

To access **History**:

- web client: Navigate to **Security Policy Management** > **User Groups** > (Edit) > **History** or **User Management** > **User Groups** > (Edit) > **History**.

  The top of the **History** tab contains the following information:

  - **Date Range**: By default, the history details are displayed for the last 24 hours. From the drop-down, select one of the time intervals to display history details for that time frame.
  - **Export**: Use this button to export the listed data as either a JSON or CSV file. For more information, see Exporting data.
  - **Refresh**: Update the list displayed.
  - **Search**: For more information, see Search box on page 78.

Table 233: User Groups: History tab properties

Property	Description
Date/Time	The date and time of the event
User	The display name of the user that triggered the event
Source IP	The network DNS name or IP address of the managed system that triggered the event
Object Name	The name of the selected group
Event	The type of operation made to the selected user group: • Create • Delete • Update • Add Membership • Remove Membership • Directory Group Sync Complete NOTE: A membership operation indicates a relationship change with a related or parent object such as a user was added or removed from the membership of the selected user group or the selected group was added or removed from an entitlement.

Property	Description
Related Object	The name of the related object
Related Object Type	The type of the related object
Parent	The name of the object to which the selected user group is a child
Parent Object Type	The parent object type

Managing user groups

Use the controls and tabbed pages on the User Groups page to perform the following tasks to manage SPP user groups:

- Adding a user group
- Adding a directory user group
- Adding a SCIM user group
- Adding users to a user group
- Adding a user group to an entitlement
- Deleting a user group

Adding a user group

It is the responsibility of the Security Policy Administrator, Authorizer Administrator, and User Administrator to add groups of users to SPP.

To add a user group

1. Navigate to **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. Click **+ New User Group** from the toolbar and select **User Group**.
3. In the **New User Group** dialog, enter the following information:
   a. **Name**: Enter a unique name for the user group.

      Limit: 50 characters

   b. **Description**: (Optional) Enter information about this user group.

      Limit: 255 characters
4. On the **Permissions** tab, select **Help Desk** and/or the **Personal Password Vault** permission to be assigned to each member of the **Group**. For each group member, the selected permissions of the Group will be combined with any existing permissions that have already been granted explicitly or by some other Group to which they

belong. For more information, see the Permissions tab (add user).
During synchronization of a Group (which occurs every 15 minutes), a user may be identified as no longer being a member. In this case, the selected permissions of the Group are removed from the user unless the user is also a member of another Group from which they inherit the permission. SPP does not keep track of nor distinguish between an explicitly assigned permission versus one that was assigned via a Group.

> IMPORTANT: The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Groups from which they inherited it, the user will no longer be able to access **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission again, they regain access to all of their existing data.

5. Click **OK**. On an import, the user group is created and the assigned users appear when the import process is complete.

Adding a directory user group

In order to add a directory user group, an Appliance Administrator must add an Active Directory or LDAP server as an identity provider.

- web client: Navigate to **Appliance Management** > **Safeguard Access** > **Identity and Authentication**.

  For more information, see Identity and Authentication on page 254.

Next, the Authorizer Administrator or the User Administrator can add directory user groups.

The Security Policy Administrator, Authorizer Administrator, and User Administrator can add local user groups. For more information, see Adding a user group on page 555.

Import consideration

All users who are part of a directory import user group must have complete and valid attributes. If the attributes for a user are not complete and valid, the user is not imported and the import continues.

Port

The standard global catalog port, 3268 (LDAP), must be open on the firewall for every Windows global catalog server in the environment and SPP Appliance to communicate for directory management tasks (for example, adding a directory account, a directory user account, or a directory user group). LDAP uses port 389 for unencrypted connections. For more information, see the Microsoft publication How the Global Catalog Works.

Time

Because Microsoft Active Directory does not have a Time Zone attribute, when you add a directory group, the default time zone is set for all imported accounts to (UTC) Coordinated Universal Time. To reset the time zone, open each imported account in **Users** and modify the Time Zone on the **Location** tab.

To add a directory user group

1. Navigate to **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. Click **+ New User Group** from the toolbar and select **Directory User Group**.
3. In the **Directory Group** tab:
   a. Select a directory.
   b. For **Filter Search Location**, use **Browse** to select a container within the directory. This option is not available for Starling directories.
   c. The **Include objects from sub containers** check box is selected by default indicating that child objects will be included in your search. Clear this check box to exclude child objects from your search. This option is not available for Starling directories.
   d. In the **Contains** field, enter a full or partial directory group name and click **Search**. Or leave blank to return the first 1,000 items.

      The text search is not case-sensitive and does not allow wild cards. SPP searches each domain of a forest. You can search on partial strings. For example, if you enter "ad" in the search box, it will find any directory group that contains "ad."
   e. Select a group name from the results displayed in the **Select the group to add** grid.
   f. At the bottom of the **Directory Group** dialog, select the **Automatically link Managed Directory Accounts** check box to have existing managed directory accounts set as linked accounts on the imported user. This option is not available for Starling directories.

      Based on the setting of the identity provider's Managed Objects attribute, the attribute values are used to match up with existing managed directory accounts in Safeguard. The Safeguard user's set of linked accounts will periodically synchronize with the directory and be overwritten with the values from the directory. Any changes to the linked accounts made manually to the user are lost at the next directory synchronization (see **Sync additions every** under Management tab (add asset)).
4. In the **Authentication** tab, set the primary and secondary authentication. If you are importing users, Safeguard sets the primary and secondary authentication providers for new users. If a directory user group member already exists as a user in Safeguard, their authentication properties are not changed. To change authentication settings on existing Safeguard users that are members of the group, you must manually invoke the `/UserGroups/{id}/SynchronizeAndUpdateProviders`

API method.
Directory groups require the forest root domain to be visible and available for identity and authentication set on **Appliance Management** > **Safeguard Access** > **Identity and Authentication**. For more information, see Available Domains for Identity and Authentication (for Active Directory) on page 261.

a. The **Authentication Provider** field defaults to the directory (or the forest root name for Active Directory) from which the group came.

   All newly created Safeguard users that are imported from the directory user group will have their primary authentication provider set to use the directory domain from which their user originates. For an Active Directory forest with multiple domains, the domains must be marked as **Available Domains for Identity and Authentication**. If a user is a member of a group, but their domain is not marked as **Available for Identity and Authentication**, the user will not be imported. For more information, see Adding identity and authentication providers on page 259.

   You can use either an External Federation or Radius server as each user's primary authentication provider. During an import process, the directory attribute that was specified for **External Federation Authentication** or **Radius Authentication** will be used to set the user's **Email Address** or **Name Claim** (for External Federation) or **Login name** (for Radius) property. See the External Federation settings attribute and Radius settings attribute for more information.

b. Select the **Require Certificate Authentication** check box to require that the user logs in to Safeguard using their domain issued user certificate or SmartCard. This option is only available when the directory user group comes from Microsoft Active Directory and the **Authentication Provider** is also set as that directory.

c. You can require the user to log in with two-factor authentication. Users being imported must have their contact information complete in order to successfully create a user in Safeguard.

   i. Select the **Require Secondary Authentication** check box. For more information, see Requiring secondary authentication log in on page 546.

   ii. Choose the secondary **Authentication Provider** for all users of the directory user group. Use valid combinations of identity and authentication providers. For more information, see Identity and Authentication on page 254.

5. On the **Permissions** tab, select any of the administrative permissions and/or the **Personal Password Vault** permission to be assigned to each member of the **Directory Group**. For each group member, the selected permissions of the group will be combined with any existing permissions that have already been granted explicitly or by some other Group to which they belong. For more information, see the Permissions tab (add user).
During synchronization of a Directory Group, a user may be identified as no longer

being a member. In this case, the selected permissions of the Directory Group are removed from the user unless the user is also a member of another Group from which they inherit the permission. SPP does not keep track of nor distinguish between an explicitly assigned permission versus one that was assigned via a Group.

> IMPORTANT: The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Groups from which they inherited it, the user will no longer be able to access **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission again, they regain access to all of their existing data.

6. Click **OK**. On an import, the directory user group is created and the assigned users appear when the import process is complete.
7. After adding the information, you can edit the following directory group settings and the directory synchronization process will be triggered in the background.
   - **Directory Group** tab: Select or clear the **Automatically link Managed Directory Accounts** check box.
   - **Authentication** tab: Change the authentication providers.

     > NOTE: Changing the authentication providers will only effect newly imported users. Existing users will not have their authentication providers updated. To change authentication settings on existing Safeguard users that are members of the group, you must manually invoke the `/UserGroups/{id}/SynchronizeAndUpdateProviders` API method.
   - **Permissions** tab: Change the permissions.

Adding a SCIM user group

In order to add a SCIM user group, you must first configure SCIM provisioning. For more information on configuring SCIM provisioning, see Adding identity and authentication providers.

Next, the Authorizer Administrator or the User Administrator can add SCIM user groups.

To add a SCIM user group

1. Navigate to **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. Click **+ New User Group** from the toolbar and select **SCIM User Group**.
3. In the **SCIM Group** dialog, enter the following information:
   a. **Identity Provider**: Select the SCIM identity provider.
   b. **Name**: Enter a unique name for the user group.
   c. Limit: 50 characters

d. **Description**: (Optional) Enter information about this user group.

e. Limit: 255 characters

4. On the Authentication tab, select the Authentication Provider.
5. (Optional) Select the **Require Secondary Authentication** check box. For more information, see Requiring secondary authentication log in on page 546.
6. On the **Permissions** tab, select any of the administrative permissions and/or the **Personal Password Vault** permission to be assigned to each member of the **SCIM User Group**. For each group member, the selected permissions of the group will be combined with any existing permissions that have already been granted explicitly or by some other Group to which they belong. For more information, see the Permissions tab (add user).
   During synchronization of a SCIM User Group, a user may be identified as no longer being a member. In this case, the selected permissions of the SCIM User Group are removed from the user unless the user is also a member of another Group from which they inherit the permission. SPP does not keep track of nor distinguish between an explicitly assigned permission versus one that was assigned via a Group.

   > IMPORTANT: The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Groups from which they inherited it, the user will no longer be able to access **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission again, they regain access to all of their existing data.
7. Click **OK**.
8. After adding the information, you can edit the following SCIM User Group settings and the synchronization process will be triggered in the background.
   - **SCIM Group** tab: Change the identity provider.
   - **Authentication** tab: Change the authentication providers.

     > NOTE: Changing the authentication providers will only effect newly imported users. Existing users will not have their authentication providers updated. To change authentication settings on existing Safeguard users that are members of the group, you must manually invoke the `/UserGroups/{id}/SynchronizeAndUpdateProviders` API method.
   - **Permissions** tab: Change the permissions.

Adding users to a user group

It is the responsibility of an Authorizer Administrator, User Administrator, or Security Policy Administrator to add users to local SPP groups. For directory user groups, you cannot manually add or remove users. Instead, those groups will automatically be synchronized with the Active Directory or LDAP server they came from.

To add users to a user group

1. Navigate to:
   - web client: **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. In **User Groups**, select a user group from the object list and open the **Users** tab.
3. Click **+ Add User** from the details toolbar.
4. Select one or more users from the list in the **Users** dialog and click **OK**.

   IMPORTANT: You cannot add a group to a user group's membership; group membership cannot be nested.

Adding a user group to an entitlement

When you add user groups to an entitlement, you are specifying which people can request access to the accounts and assets governed by an entitlement's policies. It is the responsibility of the Security Policy Administrator to add user groups to entitlements.

To add a user group to entitlements

1. Navigate to:
   - web client: **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. In **User Groups**, select a user group from the object list and open the **Entitlements** tab.
3. Click **+ Add Entitlement** from the details toolbar.
4. Select one or more entitlements from the **Entitlements** dialog and click **OK**.

Deleting a user group

Both Authorizer Administrator and User Administrator can delete local and directory user groups. A Security Policy Administrator can only delete local groups without permissions on them.

When you delete a user group, SPP does not delete the users associated with it.

To delete a user group

1. Navigate to:
   - web client: **Security Policy Management** > **User Groups** or **User Management** > **User Groups**.
2. In **User Groups**, select a user group from the list.

3. Click 🗑 **Delete**.
4. Confirm your request.

Time Zone

SPP sets a default time zone based on the location of the person performing the set up. The time zone is expressed as UTC + or – hours:minutes and is used for timed access (for example, access from 9 a.m. to 5 p.m.). It is recommended that the Bootstrap Administrator set the desired time zone on set-up. An Authorizer Administrator can also change the time zone.

To configure the time zone

1. Navigate to **User Management** > **Settings** > **Time Zone**.
2. The User Administrator can search for and select the desired time zone.
3. The User Administrator can change **Allow users to modify their own time zone**.
    - Enable the setting to let users change their time zone (the default).
    - Disable the setting to prohibit a user from changing their time zone, possibly to ensure the user conforms with policy.

14

Reports

Reports allows users to view and export reports that show which assets, accounts, users, tags, and partitions a selected user manages. Reports can be exported in .csv or .json format.

In the web client, the **Reports** section contains the following sub-pages:

- Activity Center: The **Activity Center** is the place to go to view the details of specific events or user activity. The appliance records all activities performed within One Identity Safeguard for Privileged Passwords. Any administrator has access to the audit log information; however, your administrator permission set determines what audit data you can access.
- **Entitlements**: One Identity Safeguard for Privileged Passwords provides the following types of entitlement reports (for more information, see Entitlement reports):

  NOTE: The number indicated in the tab title shows the number of unique users, assets, or accounts. When you enter search criteria for the report, the number displayed on the tab will adjust accordingly.

  - **User**: Lists information about the accounts a selected user is authorized to request.
  - **Asset**: Lists information about the accounts associated with a selected asset and the users who have authorization to request those accounts.
  - **Account**: Lists detailed information about the users who have authorization to request a selected account including: Entitlement, Policy, Access Type, Password Included, Password Change, Time Restrictions, Expiration Date, Group, From Linked Account, and Last Accessed.
- **Ownership**: One Identity Safeguard for Privileged Passwords provides these ownership reports (for more information, see Ownership reports):

  NOTE: The number indicated in the tab title shows the number of unique users, partitions, assets, accounts, or tags. When you enter search criteria for the report, the number displayed on the tab will adjust accordingly.

  - **User**: Lists information about ownership based on each owner.
  - **Partition**: Lists information about ownership for a partition.
  - **Asset**: Lists information about ownership for an asset.

- **Account**: Lists information about ownership for an account.
- **Tag**: Lists information about owners of assets and accounts assigned to a tag.

Activity Center

The **Activity Center** is the place to go to view the details of specific events or user activity. The appliance records all activities performed within One Identity Safeguard for Privileged Passwords. Any administrator has access to the audit log information; however, your administrator permission set determines what audit data you can access. For more information, see Administrator permissions on page 604.

Activity Center

The **Activity Center** page contains these options:

- **Select a Saved Search**: Allows you to access and manage previously saved search and scheduled reports.
- **Save or Schedule Search**: Saves the current search criteria which can be used later to generate the report. For more information, see Saving search criteria and loading previously saved search criteria on page 566.
- **Clear Search Criteria**: Resets the current search criteria back to the default settings (all activity occurring within the last 24 hours).
- **Activity Category**: Use this drop-down to filter the activity being searched for based on category. Selecting **All Activity** will search all categories.
- **Date Range**: Use this drop-down to specify a time frame for the search.

Use the available search fields to specify additional query criteria to retrieve the information you are looking for. For more information, see Applying search criteria on page 565.

Activity Center: Results toolbar

Once an activity audit log report is generated, the results section contains the search results grid and these toolbar options:

- **View Details**: After selecting a result, click this button to view the details.
- **Request Workflow Details**: After selecting a result related to an access request, click this button to open a detail of all actions for that request (for example: approvals, password checkouts, and session logs).
- **Export**: Select to create a .csv or .json file of the criteria displayed and save it to a location of your choice.

- **Refresh**: Updates the search results page.
- **Search**: You can search by a character string or by a selected attribute with conditions you enter. To search by a selected attribute click **Search** and select an attribute to search. For more information, see Search box on page 78.

Applying search criteria

Use the query builder in the **Activity Center** to add and remove data from your activity audit log report to get the information you need.

By default, an activity audit log report includes all activity occurring within the last 24 hours. However, using the query options provided you can specify search criteria to retrieve specific information from the activity audit log. The available search criteria may include:

- **Activity Category**: Use this drop-down to narrow parameters and event details.
- **Date Range**: Use this drop-down to narrow results by hours, days, or a custom time frame you set.
- **User Name**: Clicking this field opens a dialog where you can select a user for the activity report.
- **Asset Name**: Clicking this field opens a dialog where you can select the asset for the activity report.
- **Account Name**: Clicking this field opens a dialog where you can select the account for the activity report.

To apply search criteria to the audit log

Activity Category and Time frame are required to generate a report. Other search criteria is optional and allows you to narrow the report to the exact parameters provided.

1. Navigate to the **Activity Center** (**Reports** > **Activity Center**).
2. **Activity Category** defaults to **All Activity (Summary Only)**. Click the drop-down to limit the report to select the activity category to be included in the report.
3. **Date Range** defaults to **Last 24 Hours**. To specify a different time frame, click the drop-down and select the time frame to be included in the report. If using the **Custom** option, specify the custom date and time range.
4. Clicking the **User Name** field opens a dialog where you can select a user for the activity report.
5. When available, clicking the **Asset Name** field opens a dialog where you can select the asset for the activity report.
6. When available, clicking the **Account Name** field opens a dialog where you can select the account for the activity report.

7. To remove your selections, use **Clear Search Criteria** to reset the search back to the default.

Saving search criteria and loading previously saved search criteria

You can save the current search criteria defined to be used at a later time to generate an activity audit log report. You can save the current search criteria from the main Activity Center view (query builder page) or from the results view.

To save the current search criteria

1. Navigate to the **Activity Center** (**Reports** > **Activity Center**).
2. Specify the search criteria to be used to generate the desired report. For more information, see Applying search criteria on page 565.
3. Click **Save or Schedule Search**.
4. In the **Save Scheduled Report** dialog, enter the following information:
   a. **Name**: Enter a name for the search.
   b. **Description**: Optionally, enter descriptive text to describe the search.
   c. **Run Every**: By default this is set to **Never**. Selecting another option from the drop-down will enable additional configuration options. For more information, see Scheduling an activity audit log report
5. Click **OK**.
6. To run a previously saved search, click **Select a Saved Search**.
   a. Select a search from the list.
   b. Click **OK**.

   The search criteria for the selected search appears on the Activity Center page.

To load previously saved search criteria

1. Navigate to the **Activity Center** (**Reports** > **Activity Center**).
2. Click **Select a Saved Search**.
3. Select a search from the list.
4. Click **Load Report**.

   The search criteria for the selected search appears on the Activity Center page.

Generating an activity audit log report

To generate an activity audit log report

1. Navigate to the **Activity Center** (**Reports** > **Activity Center**).
2. Use the query options provided to specify the content of the report. By default the audit log returns all activity occurring within the last 24 hours. For more information, see Applying search criteria on page 565.
3. The information displayed by default depends on the type of activity report generated. You can change the columns displayed by selecting the **Columns** in the upper right of the results list.

Actions once a report is generated

Once a report is generated, you can use the buttons above the grid as described below.

- **View Details**: After selecting a result, click this button to open a detailed summary.
- **Request Workflow Details**: Select an access request event and click **Workflow** to audit the transactions that occurred during the request's workflow from request to approval to review. For session requests, you can also replay a recorded session or live session from the **Request Workflow** dialog.
- **Export**: Click to export the data as CSV or JSON to the location of your choice. Different information may be returned based on whether you select CSV or JSON. For example, JSON includes details of accounts discovered and CSV includes only the count of accounts. For more information, see Exporting data. The time is set according to the user time zone.
- **Refresh**: Closes the details and updates the search results page.
- **Column**: Select to display a list of columns that can be displayed in the grid. Select the check box for data to be included in the report. Clear the check box for data to be excluded from the report. The additional columns available depend on the type of activity included in the report.

Scheduling an activity audit log report

SPP allows you to schedule the generation of an activity audit log report, which will then be sent via email. The emailed report will be an attachment in the selected .csv or .json format.

To schedule an activity audit log report

1. Navigate to the **Activity Center** (**Reports** > **Activity Center**).
2. Use the query options provided to specify the content of the report. By default the audit log returns all activity occurring within the last 24 hours. For more information, see Applying search criteria on page 565.
3. Click **Save or Schedule Search**.
4. In the **Save Scheduled Report** dialog, enter the following information:
   a. **Name**: Enter a name for the report.
   b. **Description**: Optionally, enter descriptive text for the report.
   c. To set the schedule, use the following options:
      - Select a time frame:
        - **Never**: The job will not run according to a set schedule. You can still manually run the job.
        - **Minutes**: The job runs per the frequency of minutes you specify. For example, `Run Every 30/Minutes` runs the job every half hour over a 24-hour period. It is recommended you do not use the frequency of minutes except in unusual situations, such as testing.
        - **Hours**: The job runs per the minute setting you specify. For example, if it is 9 a.m. and you want to run the job every two hours at 15 minutes past the hour starting at 9:15 a.m., select `Run Every 2/Hours/@ minutes after the hour 15`.
        - **Days**: The job runs on the frequency of days and the time you enter.

          For example, `Run Every 2/Days/Starting @ 11:59:00 PM` runs the job every other evening just before midnight.
        - **Weeks** The job runs per the frequency of weeks at the time and on the days you specify.

          For example, `Run Every 2/Weeks/Starting @ 5:00:00 AM` and **Repeat on these days** with **MON**, **WED**, **FRI** selected runs the job every other week at 5 a.m. on Monday, Wednesday, and Friday.
        - **Months**: The job runs on the frequency of months at the time and on the day you specify.

          For example, If you select `Run Every 2/Months/Starting @ 1:00:00 AM` along with `Day of Week of Month/First/Saturday`, the job will run at 1 a.m. on the first Saturday of every other month.
      - Select **Use Time Windows** if you want to enter the **Start** and **End** time.

        You can click **+ Add** or **− Remove** to control multiple time restrictions. Each time window must be at least one minute apart and not overlap.

For example, for a job to run every ten minutes every day from 10 p.m. to 2 a.m., enter these values:

Enter `Run Every 10/Minutes` and set **Use Time Windows**:

- **Start 10:00:00 PM** and **End 11:59:00 PM**
- **Start 12:00:00 AM** and **End 2:00:00 AM**

  An entry of **Start 10:00:00 PM** and **End 2:00:00 AM** will result in an error as the end time must be after the start time.

If you have selected **Days**, **Weeks**, or **Months**, you will be able to select the number of times for the job to **Repeat** in the time window you enter.

For a job to run two times every other day at 10:30 am between the hours of 4 a.m. and 8 p.m., enter these values:

For days, enter `Run Every 2/Days` and set **Use Time Windows** as **Start 4:00:00 AM** and **End 8:00:00 PM** and **Repeat 2**.

If the scheduler is unable to complete a task within the scheduled interval, when it finishes execution of the task, it is rescheduled for the next immediate interval.

5. **Fields**: Clicking this button opens a dialog where you can select which fields will be included in the results.
6. **Sort By**: Clicking this button opens a dialog where you can select the sort order for the selected fields.
7. **Report Will be Sent To**: Read-only field displaying the email address of the user currently logged into the SPP client. This field is required. If this field is blank, you must set your email address in **My Account**.
8. Select a **Report Format**, which can be **CSV** or **JSON**. Different information may be returned based on whether you select CSV or JSON. For example, JSON includes details of accounts discovered and CSV includes only the count of accounts.
9. Select the **Detailed Report (Not Valid for All Activity)** check box to generate a longer, more detailed report.
10. Click **OK**.

Editing or deleting a saved search or scheduled report

To edit or delete a saved search or scheduled report

Click the **Select a Saved Search** toolbar button to display a list of saved searches and scheduled reports. From this dialog, you can locate, delete, or edit a saved search or scheduled report.

1. Navigate to the **Activity Center** (**Reports** > **Activity Center**).
2. Click **Select a Saved Search**. The **Select a Saved Search** dialog displays, which contains a list of all saved searches and scheduled reports.
3. Select a saved search or scheduled report from the list.
4. Click one of the toolbar buttons.
   - **Delete** then click **Yes** in the confirmation dialog to delete the saved search.
   - **Edit** to display the **Save Scheduled Report** to modify the name and description for a saved search. You can also modify the schedule settings for a scheduled report.
   - **Refresh** to refresh the list.

NOTE: After selecting a search, double-click or click the **Load report** button to close the **Select a Saved Search** dialog and display the search results.

Viewing event details

Additional detailed information is available for some activity events.

To see the details of a specific event

1. Use one of the following method to view event details:
   - Double-click an event.
   - Select an event and click **View Details**.
2. To close the event details pane, click **Close**.

Auditing request workflow

In addition to reviewing activity, you can use the Activity Center to audit the transactions that occurred during the request workflow process, from request to approval to review. For session requests, you can also play back a recorded or live session if **Record Sessions** is enabled in the entitlement's policy.

If you are an authorized reviewer, you can audit an access request's workflow of a completed request awaiting review from the Home page as well.

To audit request workflow

1. Open the **Activity Center**, use the query options to specify the content of the report.
2. Select an access request event and click **Request Workflow Details** to audit the transactions that occurred during the request's workflow from request to approval to review.

3. For session requests that have **Record Session** enabled in the policy, click the button to access event session logs via Safeguard for Privileged Sessions.

Sorting report results

Use the controls in the grid heading row to sort report results or rearrange the columns of data. An arrow in the column heading identifies the sort criteria and order, ascending or descending, being used to display information.

To sort columns

1. Click the column heading to be used for the sort criteria.
2. The sort order is in ascending order. To change it to descending order, click the heading a second time.

To change the columns that display

In the upper right corner, click **Column** to see a list of columns that can be displayed in the grid. Select the check box for data to be included in the report. Clear the check box for data to be excluded from the report. The additional columns available depend on the type of activity included in the report.

Entitlement reports

Security Policy Administrators, Auditors, and Application Auditors can run an entitlement report.

To export the data from an Entitlement report

1. Navigate to **Reports** > **Entitlements**.
2. From the top of the Entitlements page, select the tab for **User**, **Asset**, or **Account**.

   NOTE: The number indicated in the tab title shows the number of unique users, assets, or accounts. When you enter search criteria for the report, the number displayed on the tab will adjust accordingly.
3. (Optional) Apply any desired filters to the table.
4. You can then select to either export the data for all listed items or the data for a single item:
   - To export data for all items, select **Export** on the toolbar.
   - To export data for a single item, select an item and click **View Details**. From the details dialog, select **Export**.

5. From the Export dialog, select to export the data as either a JSON or CSV file. For more information, see Exporting data. The time is set according to the user time zone.
6. Click **Export** to generate the report file.

Exporting a detailed user entitlement report

Security Policy Administrators, Auditors, and Application Auditors can export a user entitlement report that also includes detailed information on each of the associated accounts.

To export a detailed user entitlement report

1. Navigate to **Reports** > **Entitlements**.
2. From the top of the Entitlements page, select the **User** tab.

   NOTE: The number indicated in the tab title shows the number of unique users. When you enter search criteria for the report, the number displayed on the tab will adjust accordingly.
3. (Optional) Apply any desired filters to the table.
4. Click the button to export a CSV file containing the data.

Ownership reports

Asset Administrators, Auditors, and Application Auditors can run an ownership report.

To export the data from an Ownership report

1. Navigate to **Reports** > **Ownership**.
2. From the top of the Entitlements page, select the tab for **User**, **Asset**, **Account**, **Partition**, or **Tag**.

   NOTE: The number indicated in the tab title shows the number of unique users, partitions, assets, accounts, or tags. When you enter search criteria for the report, the number displayed on the tab will adjust accordingly.
3. (Optional) Apply any desired filters to the table.
4. You can then select to either export the data for all listed items or the data for a single item:

- To export data for all items, select **Export** on the toolbar.
- To export data for a single item, select a listed item and click **View Details**. From the details dialog, select **Export**.

5. From the Export dialog, select to export the data as either a JSON or CSV file. For more information, see Exporting data. The time is set according to the user time zone.
6. Click **Export** to generate the report file.

15

Disaster recovery and clusters

SPPAppliances can be clustered to ensure high availability. Clustering enables the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. This reduces down time and data loss.

Another benefit of clustering is load distribution. Clustering in a managed network ensures the load is distributed to ensure minimal cluster traffic and to ensure appliances that are closest to the target asset are used to perform the task. The Appliance Administrator defines managed networks (network segments) to effectively manage assets, account, and service access requests in a clustered environment to distribute the task load.

Primary and replica appliances

A SPP cluster consists of three or five appliances. An appliance can only belong to a single cluster. One appliance in the cluster is designated as the primary. Non-primary appliances are referred to as replicas. All vital data stored on the primary appliance is also stored on the replicas. In the event of a disaster, where the primary appliance is no longer functioning, you can promote a replica to be the new primary appliance. Network configuration is done on each unique appliance, whether it is the primary or a replica.

The replicas provide a read-only view of the security policy configuration. You cannot add, delete, or modify the objects or security policy configuration on a replica appliance. On the replica; you can perform check and change operations for passwords and ssh keys, set password, and set ssh key (both imported and generated). Users can log in to replicas to request access, generate reports, or audit the data. Also, passwords, SSH keys, and sessions can be requested from any appliance in a Safeguard cluster.

Supported cluster configurations

Current supported cluster configurations follow.

- 3 Node Cluster (1 Primary, 2 Replicas): Consensus is achieved when two of the three appliances are online and able to communicate. Valid states are: Online or ReplicaWithQuorum. For more information, see Appliance states on page 599.
- 5 Node Cluster (1 Primary, 4 Replicas): Consensus is achieved when three of the five appliances are online and able to communicate. Valid states are: Online or ReplicaWithQuorum. For more information, see Appliance states on page 599.

Consensus and quorum failure

Some maintenance tasks require that the cluster has consensus (quorum). Consensus means that the majority of the members (primary or replica appliances) are online and able to communicate. Valid states are: Online or ReplicaWithQuorum. For more information, see Appliance states on page 599.

Supported clusters have an odd number of appliances so the cluster has a consensus equal to or greater than 50% of the appliances are online and able to communicate.

If a cluster loses consensus (also known as a quorum failure), the following automatically happens:

- The primary appliance goes into Read-only mode.
- Password and SSH key check and change is disabled.

When connectivity is restored between a majority of members in a cluster, consensus is automatically regained. If the consensus members include the primary appliance, it automatically converts to read-write mode and enables password and SSH key check and change.

Health checks and diagnostics

The following tools are available to perform health checks and diagnose the cluster and appliances.

- Perform a health check to monitor cluster health and appliance states. For more information, see Maintaining and diagnosing cluster members on page 580.
- Diagnose the cluster and appliance. You can view appliance information, run diagnostic tests, view and edit network settings, and generate a support bundle. For more information, see Diagnosing a cluster member on page 588.
- If you need to upload a diagnostic package but can't access the UI or API, connect to the Management web kiosk (MGMT). The MGMT connection gives access to functions without authentication, such as pulling a support bundle or rebooting the appliance, so access should be restricted to as few users as possible.

Shut down and restart an appliance

You can shut down and restart an appliance.

- Shut down an appliance. For more information, see Shutting down the appliance on page 128.
- Restart an appliance. For more information, see Restarting the appliance on page 129.

Run access request workflow on an isolated appliance in Offline Workflow Mode

You can enable Offline Workflow Mode either automatically or manually to force an appliance that no longer has quorum to process access requests using cached policy data in isolation from the remainder of the cluster. The appliance will be in Offline Workflow Mode.

- For general information on Offline Workflow Mode, see About Offline Workflow Mode.
- To manually enable offline workflow or manually resume online workflow, see Manually control Offline Workflow Mode.
- To configure automatic Offline Workflow Mode and, optionally, automatically Resume Online Workflow, see Offline Workflow (automatic). When automation is turned on, you can still also manually control Offline Workflow Mode.

Primary appliance failure: failover and backup restore

If a primary is not communicating, perform a manual failover. If that is not possible, you can use a backup to restore an appliance.

- Failover: If the primary is not communicating, you can perform a manual failover if there is a quorum (the majority has consensus). For more information, see Failing over to a replica by promoting it to be the new primary on page 587.
- Backup restore: Perform a backup restore if no appliance can be restored using failover. For more information, see Using a backup to restore a clustered appliance on page 591.

Unjoin and activate

If the cluster appliances are able to communicate, you can unjoin the replica, then activate the primary so replicas can be joined.

- You can unjoin a replica in any state and place it in Standalone Read-only mode (StandaloneReadOnly state). For more information, see Unjoining replicas from a cluster on page 578.
- You can activate an appliance that has been been unjoined and placed in Standalone Read-only mode (StandaloneReadOnly state) if the appliance is not managed in anther Safeguard cluster. For more information, see Activating a read-only appliance on page 588.

Cluster reset

If the appliance is offline or the cluster members are unable to communicate, you must use **Cluster Reset** to rebuild the cluster. If there are appliances that must be removed from the cluster but there is no quorum to safely unjoin, a cluster reset force-removes nodes from the cluster. For more information, see Resetting a cluster that has lost consensus on page 593.

Factory reset

Perform a factory reset to recover from major problems or to clear the data and configuration settings on a hardware appliance. All data and audit history is lost and the hardware appliance goes into maintenance mode.

You can perform a factory reset from:

- The Recovery Kiosk. For more information, see Factory reset from the Recovery Kiosk on page 651.
- The virtual appliance Support Kiosk. For more information, see Support Kiosk on page 56.

Enrolling replicas into a cluster

Prior to the Appliance Administrator enrolling cluster members into a SPP cluster, review the enrollment considerations that follow.

Considerations to enroll cluster members

- If there is an appliance in Offline Workflow Mode, resume online operations before adding another replica. For more information, see About Offline Workflow Mode on page 581.
- Update all appliances to the same appliance build (patch) prior to building your cluster. During the cluster patch operation, access request workflow is available so authorized users can request password and SSH key releases and session access.
- To enroll an appliance into a cluster, the appliance must communicate over port 655 UDP and port 443 TCP, and must have IPv4 or IPv6 network addresses (not mixed). If both IPv4 and IPv6 are available for the connection then IPv6 will be used.For more information, see Safeguard ports on page 676.
- You can only enroll replica appliances to a cluster when logged in to the primary appliance (using an account with Appliance Administrator permissions).
- You can only add one appliance at a time. The maintenance operation must be complete before adding additional replicas.
- Enrolling a replica can take as little as five minutes or as long as 24 hours depending on the amount of data to be replicated and your network.
- During an enroll replica operation, the replica appliance goes into Maintenance mode. The existing members of the cluster can still process access requests as long as the member has quorum. On the primary appliance, you will see an enrolling notice in the status bar of the cluster view, indicating that a cluster-wide operation is in progress. This cluster lock prevents you from doing additional maintenance activities.

  Once the maintenance operation (enroll replica operation) is complete, the diagram in the cluster view (left pane) shows the link latency on the connector. The appliances in the cluster are unlocked and users can once again use the features available in SPP.

  > TIP: The Activity Center contains events for the start and the completion of the enrollment process.

- The primary appliance's objects and security policy configuration are replicated to all replica appliances in the cluster. Any objects (such as users, assets, and so on) or security policy configuration defined on the replica will be removed during enroll. Existing configuration data from the primary will be replicated to the replica during the enroll. Future configuration changes on the primary are replicated to all replicas.

To enroll a replica

1. It is recommended that you make a backup of your primary appliance before enrolling replicas to a cluster.
2. Log in to the primary appliance as an Appliance Administrator.
3. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
4. Click **+ Add Replica** to join a SPP Appliance to a cluster.
5. In the **Add Replica** dialog, enter a network DNS name or the IP address of the replica appliance into the **Network Address** field, and click **Connect**.
6. Your web browser redirects to the login page of the replica. Log in as normal, including any two-factor authentication. After successful log in, your web browser is redirected back to the web client.
   a. Enter a valid account with Appliance Administrator permissions.
   b. In the **Add Replica** confirmation dialog, enter the words **Add Replica** and click **OK** to proceed with the operation.

   SPP displays (synchronizing icon) and (lock icon) next to the appliance it is enrolling and puts the replica appliance in Maintenance mode while it is enrolling into the cluster.

   On all of the appliances in the cluster, you will see an "enrolling" banner at the top of the cluster view, indicating that a cluster-wide operation is in progress and all appliances in the cluster are locked down.
7. View the link latency: Once the maintenance operation (enroll replica operation) is complete, click on an appliance to see the link latency. The appliances in the cluster are unlocked and users can once again make access requests.
8. Log in to the replica appliance as the Appliance Administrator.
   Notice that the appliance has a state of Replica (meaning it is in a Read-Only mode) and contains the objects and security policy configuration defined on the primary appliance.

Unjoining replicas from a cluster

SPPallows the Appliance Administrator to unjoin replica appliances from a cluster. Prior to unjoining a replica from a SPP cluster, review the unjoin considerations that follow.

Considerations to unjoin cluster members

- You can only unjoin replica appliances from a cluster.
- To promote a replica to be the new primary and then unjoin the 'old' primary appliance, you can use the **Failover** option if the cluster has consensus (the majority of the appliances are online and able to communicate). For more information, see Failing over to a replica by promoting it to be the new primary on page 587. If the cluster does not have consensus, use the **Cluster Reset** option to rebuild your cluster. For more information, see Resetting a cluster that has lost consensus on page 593.
- To perform an unjoin operation, the replica appliance to be unjoined can be in any state; however, the remaining appliances in the cluster must achieve consensus (online and able to communicate).
- You can unjoin a replica appliance when logged in to any appliance in the cluster that is online, using an account with Appliance Administrator permissions.
- When you unjoin a replica appliance from a cluster, the appliance is removed from the cluster as a stand-alone appliance that retains all of the data and security policy configuration information it contained prior to being unjoined. After the replica is unjoined, the appliance is placed in a Read-only mode with the functionality identified in Read-only mode functionality. You can activate an appliance in Read-only mode so you can add, delete and modify data, apply access request workflow, and so on. For more information, see Activating a read-only appliance on page 588.

To unjoin a replica from a cluster

1. Log in to an appliance in the cluster, as an Appliance Administrator.
2. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
3. In the cluster view on the left, select the replica node to be unjoined from the cluster.
4. In the details view on the right, click **Unjoin**.
5. In the **Unjoin** confirmation dialog, enter the word **Unjoin** and click **OK** to proceed.

   SPP displays (synchronizing icon) and (lock icon) next to the appliance it is unjoining and puts the replica appliance in Maintenance mode while it is unjoining from the cluster.

   Once the operation has completed, the replica appliance no longer appears.

Login during Maintenance mode

If you log in to the replica appliance while SPP is processing an unjoin operation, you will see the Maintenance mode screen. At the end of the Maintenance mode, there will be a button indicating that the unjoin operation completed successfully:

- web client: **Continue**

Maintaining and diagnosing cluster members

Maintain and diagnosis cluster members from Cluster Management:

- web client: Navigate to **Cluster** > **Cluster Management**.

When a node is selected in the Cluster view, the right of the pane displays details about the selected appliance. From this pane you can run the following maintenance and diagnostic tasks against the selected appliance.

- **Unjoin**: Click **Unjoin** to remove a replica from the cluster. For more information, see Unjoining replicas from a cluster on page 578.
- **Failover**: Click **Failover** to promote a replica to the primary appliance. For more information, see Failing over to a replica by promoting it to be the new primary on page 587.
- **Activate**: Click **Activate** to activate a read-only appliance so it can add, modify and delete data. For more information, see Activating a read-only appliance on page 588.

  CAUTION: Activating an appliance that is in Read-Only mode will take it out of the Read-only state and enable password and SSH key check and change for managed accounts. Ensure that no other SPP Appliance is actively monitoring these accounts, otherwise access to managed accounts could be lost.

- **Diagnose**: Click **Diagnose** to open the Diagnostics pane where you can perform the following:
  - View appliance diagnostics. For more information, see Appliance Diagnostics on page 126.
  - View appliance information. For more information, see Appliance Information on page 127.
  - Run diagnostic tests against the appliance. For more information, see Network Diagnostics on page 137.
  - View or edit networking settings. For more information, see Networking on page 141.
  - Perform a factory reset. For more information, see Factory Reset on page 133.
  - Check OS licensing (virtual machine only). For more information, see Operating System Licensing on page 144.
  - Update patches. For more information, see Patch Updates on page 146.
  - Power down and restart the appliance. For more information, see Power on page 147.

    - Generate a support bundle. For more information, see Support bundle on page 148.
    - View or edit time settings. For more information, see Time on page 149.
- **Check Health**: Click **Check Health** to capture and display the current state of the selected appliance.
- **Restart**: Click **Restart** to restart the selected appliance. Confirm your intentions by entering a **Reason** and clicking **Restart**.

To fix more serious issues with a cluster, you can perform additional operations depending on the state of the cluster members. Some such operations include:

- Patching cluster members
- Using a backup to restore a clustered appliance
- Performing a factory reset
- Resetting a cluster that has lost consensus
- About Offline Workflow Mode

About Offline Workflow Mode

To ensure password and SSH key consistency and individual accountability for privileged accounts, when an appliance loses consensus in the cluster, access requests are disabled. In the event of an extended network partition, the Appliance Administrator can either automatically or manually place an appliance in Offline Workflow Mode to run access request workflow on that appliance in isolation from the rest of the cluster. When the network issues are resolved and connectivity is reestablished, the Appliance Administrator can either automatically or manually resume online operations to merge audit logs, drop any in-flight access requests, and return the appliance to full participation in the cluster.

Offline workflow considerations

- In Offline Workflow Mode, an appliance functions apart from the other members of the cluster. Users can request passwords and sessions.
- Settings for Offline Workflow are set on an individual appliance.
- Suspend/Restore account does not work in Offline Workflow mode.

Passwords and SSH keys in Offline Workflow Mode

- In Offline Workflow Mode, the appliance is enabled to request, approve, and release passwords, SSH key, and sessions without a quorum, using cached policy data.
- In Offline Workflow Mode, when policy requires change after check-in, the requirement is bypassed to allow for subsequent check out. In this case, a Access Request Password or SSH Key Reset By-passed Event is generated, stating: An

`access request subsequent check out is available as password [or SSH key] reset was by-passed.`

- Password and SSH key changes will be rescheduled and will possibly complete when network connectivity is restored even while the appliance is in Offline Workflow Mode.
- Users may still request a password or SSH key from the primary or another replica on the cluster with consensus; password and SSH key check and changes works as usual. The result is that passwords or SSH keys may get out of sync on the appliance running Offline Workflow Mode. This is expected behavior and the password and SSH key will remain out of sync until the partition is healed.
- On a network partition where one or more appliances are in Offline Workflow Mode, it is possible for two individuals to have the same password and SSH key at the same time. Tying actions back to a single responsible individual is not possible. It will still be possible to identify each person that had access to the password and SSH key at the time.

Policies in Offline Workflow Mode

- Policy will be enforced as it existed at the time the appliance, now in Offline Workflow Mode, lost network connectivity to the rest of the cluster.
- Policy requiring a password and SSH key change after check-in is bypassed and subsequent check-out from the appliance in Offline Workflow Mode is allowed.
- Policy is Read-only. Therefore, update and delete configuration operations are not allowed on the appliance in Offline Workflow Mode.
- Policy changes are only allowed if directed at an online primary within the cluster. Policy changes on the online primary do not affect the appliance in Offline Workflow Mode. Once the offline workflow appliance has resumed online operations the policy changes will be distributed.

Work flow in Offline Workflow Mode

- Regular workflow approval rules apply.
- Time-based constraints and emergency access apply.
- For the few minutes the appliance is switching to or from Offline Workflow Mode, Application to Application and any command line password or SSH key-fetching operations will be suspended.
- Platform tasks (including Suspend and Restore Accounts) are disabled in Offline Workflow Mode.

User experience: Enable Offline Workflow Mode

Users that are requesting a password and SSH key in Safeguard are returned to the Home page. Password and SSH key requests prior to the switch to Offline Workflow Mode are not displayed.

- When the switch to Offline Workflow Mode starts, this message displays: ⚠ `Safeguard is switching to Offline Workflow Mode. Please wait until this`

`process is complete before proceeding with any current work`. The bottom of the Home page displays this information: `(Switching to Offline Workflow Mode...)` and `Disconnected`. If the user clicks Refresh, the banner is replaced with: `The service is unavailable`.

- When the switch to Offline Workflow Mode is complete, a banner with this information is displayed: `Safeguard is currently in Offline Workflow Mode. Previous access requests are temporarily unavailable. You may submit new requests to continue working in Offline Workflow Mode`. The bottom of the Home page displays these messages: `(Offline Workflow Mode)` and the connection status: `Connecting` then `Connected`.

Administrators can view the workflow status on the **Cluster View** pane where a message like this displays: `Offline Workflow Enabled (This appliance is running access workflow in isolation from the cluster.)` For more information, see Cluster Management on page 196.

User experience: Resume Online Operations

When the switch to Resume Online Operations has begun, this message displays: `Safeguard is returning to normal operations. Please wait until this process is complete before proceeding with any current work`. The bottom of the Home page displays this information: `(Returning to normal operations)` and `Disconnected`. Once online operations are restored, the bottom of the Home page displays this information: `Connected`.

Notifications

- The Appliance Administrator is notified when an appliance has lost consensus (quorum) via the ApplianceStateChangedEvent.
  - A primary will change from Online to PrimaryNoQuorum.
  - A replica will change from Online to one of the following:
    - ReplicaNoQuorum (connected to primary, does not have quorum)
    - ReplicaDisconnected (disconnected from primary, does not have quorum)
    - ReplicaWithQuorum (disconnected from primary, has quorum)

  For more information, see Appliance states on page 599.
- The following events can be configured for email notifications and are written to the audit log:
  - ClusterPrimaryQuorumLostEvent
  - ClusterPrimaryQuorumRestoredEvent
  - ClusterReplicaQuorumLostEvent
  - ClusterReplicaQuorumRestoredEvent
- All access request notifications are still generated.

- The Notification service identifies whether access workflow is available on an appliance via the IsPasswordRequestAvailable, IsSSHKeyRequsteAvailable, and IsSessionsRequestAvailable properties. The following API endpoint can be used to make this determination:

  ```
  https://<hostname or IP>/service/notification/v4/Status/Availability
  ```

Audit logs in Offline Workflow Mode

- Prior to network connectivity being restored, everything that happens on the appliance running in Offline Workflow Mode is only audited on that appliance.
- The audit logs merge when network connectivity is restored between the offline member and any other member in the cluster, even while in Offline Workflow Mode.
- The audit data on any cluster member operating in Offline Workflow Mode will be lost unless the appliance is returned to the cluster using the resume online operations steps.
- All cluster members that were capable of processing access and session requests must have network connectivity restored to the remainder of the cluster to ensure the cluster wide audit history is maintained.

Avoid modifications to the cluster configuration

- It is recommended that no changes to cluster membership are made while an appliance is in Offline Workflow Mode. The online operations must be automatically or manually resumed before adding or removing other nodes to ensure the appliance can seamlessly reintegrate with the cluster.

  The Appliance Administrator is advised to resume the online operations as soon as possible for individual password or SSH key accountability, policy adherence, and audit integrity.

Cluster patching is not allowed

During a cluster patch, Offline Workflow Mode cannot be triggered manually or automatically on any of the clustered appliances.

Considerations to resume online operations

- The network partition must be corrected before resuming online operations with full functionality.
- You can resume online operations of an appliance in Offline Workflow Mode without a quorum. To resume online operations, it is highly recommended that network connectivity is restored between a majority of the cluster members, including the member in Offline Workflow Mode.
- When resuming online operations, any access requests that are in flight on the appliance that is running in Offline Workflow Mode will be dropped.
- While it is possible to resume online operations if the appliance is not connected, making access requests will no longer be available.

Automatic versus manual workflow

- You can configure automatic triggering of Offline Workflow Mode and automatic resumption of online workflow. For more information, see Offline Workflow (automatic) on page 205.
- You can manually enable Offline Workflow Mode and manually resume online workflow. Manually control Offline Workflow Mode.

Manually control Offline Workflow Mode

The Appliance Administrator can manually control Offline Workflow Mode using the following steps. Manual intervention is possible when automatic Offline Workflow Mode is enabled. For more information, see Offline Workflow (automatic) on page 205.

To manually enable Offline Workflow Mode

1. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
2. In the cluster view (left pane) of the offline appliance, click the member of the cluster that is offline.
3. In the appliance details and cluster health pane (right pane), review the errors and warnings to verify the appliance has lost consensus.
4. On the offline appliance, click **Enable Offline Workflow**. (This option is only available when the appliance has lost consensus with the cluster.)

   A message like the following displays:

   ```
   This appliance will run access workflow in isolation from the cluster to
   work around loss of consensus with the cluster. Users will be able to
   request, approve and release passwords, SSH key, and sessions via this
   appliance using cached data. When connectivity is restored, you should
   resume online operations to reintegrate this appliance with the cluster and
   merge audit logs.

   Type 'Enable Offline Workflow' in the box below to confirm.

   See KB263580 for more information.
   ```
5. In the dialog, type **Enable Offline Workflow** and click **Enter**. The appliance is in Offline Workflow Mode and enters maintenance. In the Activity Center, the **Event** for the appliance goes from **Enable Offline Workflow Started** to **Enable Offline Workflow Completed**.
6. You can verify that new requests are enabled and view the following health checks on the **Cluster Management** window:
   - If there is communication to the other members in the cluster, while connected to the member in Offline Worflow mode, a message like this displays at the top of the messages: `Cluster connectivity detected`. When communication is reestablished, you can manually resume online operations to the appliance.
   - A warning icon displays next to an appliance in Offline Workflow Mode. An error icon is displayed if viewed from any other member in the cluster if the member is unable to communicate with the member in Offline Workflow Mode. At any time, you can click **Check Health** to update the information.
   - A warning message like the following will display: `Request Workflow: Access workflow on this appliance is operating in offline isolation from the cluster. This warning will persist until online operations are resumed by an Appliance Administrator.`

To manually resume online operations

Before resuming online operations, see Considerations to resume online operations.

1. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
2. In the cluster view (left pane), click the member of the cluster that is offline.
3. On the appliance in Offline Workflow Mode, click **Resume Online Operations**. (This operation is only available when the appliance is in Offline Workflow Mode.)

   A message like the following displays:

   ```
   The appliance will be reconfigured for online operations. The appliance will
   attempt to reintegrate with the cluster and merge audit logs. Refer to the to
   the Admin Guide for more information.

   Type 'Resume Online Operations' in the box below to confirm.
   ```
4. In the dialog, type in **Resume Online Operations** and click **Enter.**
5. When maintenance is complete, click **Restart**. The appliance is returned to Maintenance mode.
6. You can verify health checks on the **Cluster Management** window. If a warning icon still displays next to the appliance, select the appliance and click **Check Health** to rerun the cluster health check and display the most up-to-date health information.

Failing over to a replica by promoting it to be the new primary

SPP allows you to failover to a replica appliance by promoting it to be the new primary.

NOTE: You can promote a replica to be the new primary anytime the cluster has consensus (that is, the majority of the cluster nodes are online and able to communicate). If you have a quorum failure (that is, the majority of the cluster members do not achieve consensus), you must perform a cluster reset instead. For more information, see Resetting a cluster that has lost consensus on page 593.

To promote a replica to be the new primary in a cluster

1. log in to a healthy cluster member as an Appliance Administrator.
2. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
3. In the cluster view (left pane), select the replica node that is to become the new primary.
4. Click **Failover**.
5. In the **Failover** confirmation dialog, enter the word **Failover** and click **OK** to proceed.

During the failover operation, all of the appliances in the cluster are placed in Maintenance mode.

Once the failover operation completes, the selected replica appliance appears as the primary with a state of online. All other appliances (including the "old" primary) in the cluster appear as replicas with a state of online.

Activating a read-only appliance

Appliances that have been unjoined from a SPP cluster or restored from a backup are placed in a Read-only mode.

You can activate an appliance in Read-only mode so you can add, delete, and modify data, apply access request workflow, and so on.

The appliance in Read-only mode must be online in order to use the **Activate** task. If it is offline or the cluster does not have consensus (that is, the majority of the remaining members are offline/unable to communicate), you must use the **Cluster Reset** option to rebuild your cluster. For more information, see Resetting a cluster that has lost consensus on page 593.

CAUTION: Activating an appliance that is in Read-Only mode will take it out of the Read-only state and enable password and SSH key check and change for managed accounts. Ensure that no other SPP Appliance is actively monitoring these accounts, otherwise access to managed accounts could be lost.

To activate a read-only appliance

1. Log in to the read-only appliance as an Appliance Administrator.
2. Go to Cluster Management where the cluster view (on the left) displays one primary appliance with a yellow warning icon indicating the appliance is in a Read-only mode.
   - web client: Navigate to **Cluster** > **Cluster Management**.
3. In the cluster view (on the left), select the read-only node to be activated.
4. Click * **Activate**.
5. In the **Activate** confirmation dialog, enter the word **Activate** and click **OK** to proceed.

   The appliance's node in the cluster view (on the left) no longer displays the yellow warning icon and the state is now **Online**.

Diagnosing a cluster member

The diagnostic tools are available to an Appliance Administrator or Operations Administrator for the currently connected appliance and any other appliances (replicas) in the cluster.

To run diagnostics on a clustered appliance

1. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
2. From the cluster view (on the left) select the appliance to be diagnosed.
3. Click **Diagnose**.
4. Click **Network Diagnostics**.
5. Choose the type of test to perform and complete the steps.
   - ARP: Use Address Resolution Protocol (ARP) to discover the Interface, Internet Address, Physical Address, and Type (dynamic or static).
   - Netstat: Use netstat to display the active connection protocol, local address, foreign address, and state.
   - NS Lookup: To obtain your domain name or IP address.
   - Ping: To verify your network connectivity and response time.
   - Show Routes: To retrieve routing table information.
   - Telnet: To access remote computers over TCP/IP networks like the internet.
   - Throughput: Test throughput to other appliances in the cluster.
   - Trace Route: To obtain your router information; trace route determines the paths packets take from one IP address to another.

Patching cluster members

When an appliance update is released, apply the patch so all appliances in the cluster are on the same version. See About cluster patching for more information on how SPP handles access requests and system failures during the cluster patching process.

Prior to installing an update patch to a cluster

- Ensure all appliances in the cluster are online and healthy. Any warnings or problems should be addressed before cluster patching. The patch install process will fail if any of the cluster members are unhealthy or cannot be contacted.

  > IMPORTANT: The primary appliance orchestrates the cluster upgrade; therefore, the primary appliance must stay online and have a solid network connection with all of the replica appliances in the cluster. If this cannot be reasonably assured, you should unjoin the replica appliances from the cluster, individually upgrade them, and then re-enroll them into cluster.

- It is highly recommended to take a backup of your primary appliance before applying a patch. For more information, see Backup and Restore on page 161.
- You may want to unjoin a replica from the cluster to serve as a backup appliance. In case of a catastrophic failure, you can activate the unjoined replica to be the primary.

If the cluster patching process is successful, upgrade the unjoined replica, and then re-enroll it back into the cluster.

To patch appliances in a cluster

1. Log in to the primary appliance, as an Appliance Administrator.
2. Go to the patch updates page:
   - web client: Navigate to **Appliance** > **Patch Updates**.
3. Click **Upload a File** and browse to select an update file.

   The patch will be uploaded and distributed to all of the appliances in the cluster.

   NOTE: If you make changes to the cluster, such as adding a new replica, while a patch is staged, the update file must be distributed to the new cluster member before the patch install process can begin. SPP will not allow the patch install process to begin until all of the cluster members report that they have the update file stored locally.

   NOTE: Clicking the **Cancel** button during the distribution process stops the distribution of the update file to the replicas. At this point, you can click one of the following buttons:
   - **Remove** to remove the update file from all of the appliances in the cluster.
   - **Distribute to Cluster** to continue distributing the update file to each replica in the cluster.
4. Once the file has been successfully distributed to all of the replicas in the cluster, click the **Install Now** button.

   The primary appliance will go into Maintenance mode to begin the update operation. Once the primary appliance is successfully updated, SPP will perform the update operation on each replica, one at a time. During an update operation, the cluster will be locked so that no other cluster operations can interfere with the update operation. Once the update operation is completed on all cluster members, the cluster will automatically unlock so normal operations can resume.

   The **Cluster** view shows that an update operation is in progress and the cluster members that are locked, awaiting to install the update file. Go to:
   - web client: Navigate to **Cluster** > **Cluster Management**.

   In addition, go to Patch Updates:
   - web client: Navigate to **Appliance** > **Patch Updates**.

About cluster patching

The following information provides insight into how SPP processes access requests during the cluster patching process. It also describes what happens if a cluster member loses power or network connectivity during the patching process.

Service guarantees

During a cluster upgrade, the cluster is split logically into the current version (side A) and the upgrade version (side B). Access request workflow is only enabled on one side at a time. Audit logs run on both sides and merge when the cluster patch completes. Initially, access request workflow is only enabled on side A, and replicas in PatchPending state can perform access requests. As appliances upgrade and move to side B, the access workflow migrates to side B when side B has a majority of the appliances. At this point in the upgrade process, replicas in PatchPending state can no longer perform access requests; however, all of the upgraded cluster members can perform access requests. There is a small window where access request workflow is unavailable as the data migrates from one side to the other.

Failure scenarios

If the primary appliance loses power or loses network connectivity during the upgrade process, it will try to resume the upgrade on restart.

If a replica is disconnected or loses power during an upgrade process, the replica will most likely go into quarantine mode. The primary appliance will skip that appliance and remove it from the cluster. This replica will need to be reset, upgraded, and then re-enrolled into the cluster manually to recover.

Configuration for password and SSH key check out

The policy may be configured such that a password or SSH key reset is required before the password or SSH key can be checked out again. If that is the case, the following can be temporarily configured prior to cluster patching and access request to allow for password or SSH key check out when a password or SSH key has not been reset.

- The policy can be set to allow multiple accesses.
- The policy can be set to not require a password or SSH key change at check in.
- Emergency requests can be allowed so the user does not have to wait for the password or SSH key to be reset.

Using a backup to restore a clustered appliance

In a clustered environment, the objective of a cluster backup is to preserve and allow the restoration of all operational data, including access request workflow, users/accounts, audit logs, and so on. All appliances in a cluster (primary and replicas) can be backed up. However, a backup should only be restored to an appliance in the worst-case scenario where no appliance can be restored using the failover operation.

When a backup is restored to an appliance, the restore on the primary clears the primary's cluster configuration but does not change the replicas' cluster configuration. To avoid issues:

1. If possible, unjoin the replicas from the cluster prior to a backup restore.
2. If the primary has been set to encrypt the cluster backups with a password or GPG key, you must have the password or GPG private key to complete the upload and restore operation. For more information, see Backup protection settings on page 170.
3. Upload and restore the backup on the appliance that will be the primary.
4. If you did not unjoin the replicas prior to the backup restore, perform a cluster reset on each replica so they become standalones then join the replicas back into the cluster.

The appliance is restored as a stand-alone primary appliance in Read-only mode with no replicas. However, all the access request workflow, user/account, and audit log data that existed when the backup was taken is retained. This primary appliance can then be activated and replicas can be joined to recreate a cluster.

To take a backup of a physical appliance

1. Log in to the appliance as an Appliance Administrator.
2. Go to Safeguard Backup and Restore:
   - web client: Navigate to **Backup and Retention** > **Safeguard Backup and Restore**.
3. As needed, you can run a backup, set a schedule for the backup, and encrypt the backup for a cluster from the primary. For more information, see Backup and Restore on page 161.

To restore a physical appliance from a backup

An Appliance Administrator can restore backups as far back as SPP version 6.0.0.12276. Only the data is restored; the running version is not changed.

You cannot restore a backup from a version newer than the one running on the appliance. The restore will fail and a message like the following displays: `Restore failed because backup version [version] is newer then the one currently running [version].`

The backup version and the running version display in the Activity Center logs that are generated when Safeguard starts, completes, or fails a restore.

NOTE: If you want to use a backup file taken on a different appliance, that backup file must first be downloaded on the appliance where the backup was taken. The downloaded backup file will then need to be uploaded to the appliance that wants to use it before you can use the **Restore** option.

1. Log in to the appliance to be restored as an Appliance Administrator.
2. Go to Safeguard Backup and Restore:
   - web client: Navigate to **Backup and Retention** > **Safeguard Backup and Restore**.
3. Select the backup to be used and click **Restore**. If a problematic condition is detected, **Warning for Restore of Backup** displays along with details in the **Restore Warnings, Warning X of X** message. Click **Cancel** to stop the restore

process and address the warning or click **Continue** to move to the next warning (if any) or complete the process.

4. If the backup is protected by a password, the **Protected Backup Password** dialog displays. Type in the password in the **Enter Backup Password** text box. For more information, see Backup protection settings on page 170.
5. When the **Restore** dialog displays, enter the word **Restore** and click **OK**. For more information, see Restore a backup on page 166.

The appliance is restored as a stand-alone primary appliance in Read-only mode with no replicas.

To rebuild a cluster

1. Log in to the primary appliance as an Appliance Administrator.
2. Activate the Read-only primary appliance.
   a. Go to Cluster Management:
      - web client: Navigate to **Cluster** > **Cluster Management**.
   b. Select the node to be activated from the cluster view (left pane).
   c. Click **Activate**.
   d. Confirm the activate operation.

   For more information, see Activating a read-only appliance on page 588.
3. One at a time, enroll the replica appliances to rebuild your cluster.
   a. Go to Cluster Management:
      - web client: Navigate to **Cluster** > **Cluster Management**.
   b. Click **+ Add Replica** to join a replica appliance to the cluster.

   Once the enroll operation completes, repeat to add your appliances back into the cluster as replicas.

   NOTE: Enrolling a replica can take up to 24 hours depending on the amount of data to be replicated and your network.

   For more information, see Enrolling replicas into a cluster on page 577.

Resetting a cluster that has lost consensus

Resetting the cluster configuration allows you to recover a cluster that has lost consensus. If the cluster regains consensus after connectivity is restored, the primary will return to Read-Write mode and password and SSH key check and change will be reenabled. However, if it does not regain consensus, the Appliance Administrator must perform a cluster reset to force-remove nodes from the cluster.

If you are concerned about network issues, reset the cluster with only the new primary appliance. Once the cluster reset operation is complete, enroll appliances one by one to create a new cluster.

CAUTION: Resetting a cluster should be your last resort. It is recommended that you restore from a backup rather than reset a cluster.

Cautions

To avoid issues, consider the following cautions.

- Only reset the cluster if you are certain that consensus has been lost; otherwise, you could introduce a split-brain scenario. (Split-brain scenario is where a cluster gets divided into smaller clusters. Each of these smaller clusters believes it is the only active cluster and may then access the same data which could lead to data corruption.)
- Ensure that no cluster member has Offline Workflow Mode enabled. For more information, see Offline Workflow (automatic) on page 205.

To reset a cluster

1. Go to Cluster:
   - web client: Navigate to **Cluster** > **Cluster Management**.
2. Click the **Reset Cluster** button.

   The **Reset Cluster** dialog displays, listing the appliances (primary and replicas) in the cluster.
3. In the **Reset Cluster** dialog, select the nodes to be included in the reset operation and use the **Set Primary** button to designate the primary appliance in the cluster.

   NOTE: Nodes must have an appliance state of Online or Online Read-only and be able to communicate to be included in the reset operation. If you select a node that is not online or not available, you will get an error and the reset operation will fail.
4. Click **Reset Cluster**.
5. In the confirmation dialog, enter the words **Reset Cluster** and click **OK**.

   When connected to the new primary appliance, the Configuring SPP Appliance progress page displays, showing the steps being performed as part of the maintenance task to reset the cluster.
6. Once the maintenance tasks have completed, click **Restart**.
7. If an appliance is cluster reset as a standalone appliance, it will be placed in StandaloneReadonly mode (not online) and will require activation to avoid a split-brain scenario. For more information, see Activating a read-only appliance on page 588.

Once reset, the cluster only contains the appliances that were included in the reset operation.

Performing a factory reset

As an Appliance Administrator, you can use the Factory Reset feature to reset a SPP Appliance to recover from major problems or to clear the data and configuration settings on the appliance. A factory reset of a physical appliance may be initiated from:

- The web client
- The Recovery Kiosk
- The Support Kiosk
- Using the API

A SPP virtual appliance is reset by the recovery steps to redeploy and not a factory reset. For more information, see Virtual appliance backup and recovery on page 68.

CAUTION: Care should be taken when performing a factory reset against a physical appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. Performing a factory reset will NOT reset the BMC/IPMI interface or the IP address. However, the BMC/IPMI interface will need to be reenabled after the reset has completed (for more information, see Lights Out Management (BMC)). The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

The appliance resets to the current Long Term Support (LTS) version. For example, if the appliance is running version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, the appliance will reset down to 6.0 LTS and you will have to patch up to your desired version. For more information, see Long Term Support (LTS) and Feature Releases on page 42.

Factory reset on a clustered appliance

Performing a factory reset on a clustered hardware appliance will not automatically remove the appliance from a cluster. The recommended best practice is to unjoin an appliance from the cluster before performing a factory reset on the appliance. After the unjoin and factory reset, the appliance must be configured again. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.

To perform a factory reset from the web client

1. Go to Factory Reset on hardware (not virtual machine):
    - Navigate to **Appliance Management** > **Appliance** > **Factory Reset**.
2. Click **Factory Reset**.

3. In the Factory Reset confirmation dialog, enter the words **Factory Reset** and click **Factory Reset**.

   The appliance will go into Maintenance mode to revert the appliance. If the appliance was in a cluster, you may need to unjoin the factory reset appliance. The factory reset appliance must be configured again. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69. In addition, when you log in to the appliance, you will be prompted to add your SPP licenses.

To perform a factory reset from the Recovery Kiosk

> **CAUTION: As part of the factory reset process, you will be performing a challenge response operation.**
>
> **If the challenge response operation is invalidated, try restarting the process to generate a new challenge response. If that fails, contact One Identity Support for assistance.**

1. To perform a hardware factory reset, go to the Recovery Kiosk. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.
2. Select **Factory Reset**.
3. Press the right arrow.
4. At **Name or Email**, enter your email or name and press the **Tab** key (or down arrow).
5. Select **Submit**.
6. At **View Challenge**, press the **Enter** key. Safeguard for Privileged Passwords produces a challenge. (If the challenge is not shown, maximize Putty.)
7. Copy and paste the challenge into a text document and send it to One Identity Support. A challenge response is only good for 48 hours.

   > IMPORTANT: Do not reboot the machine during the challenge response process.

8. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select **Factory Reset**. The response is only valid for 24 hours from when it was generated by One Identity.
9. Once the factory reset is completed the appliance will need to be reconfigured.

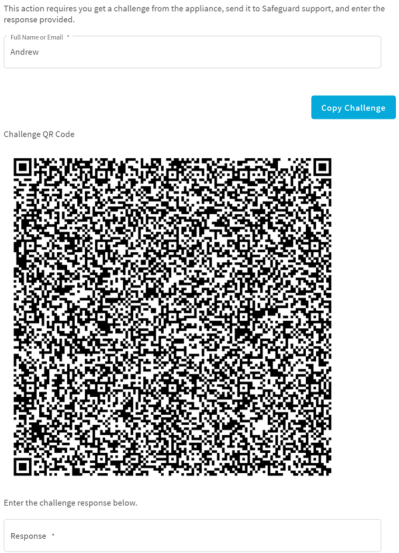
See the following Knowledge Base Article for details on using the MGMT network interface for factory reset: KB 232766: What are the steps to perform a factory reset from the recovery kiosk or MGMT network interface on physical devices?

To perform a factory reset from the Support Kiosk

> **CAUTION: As part of the factory reset process, you will be performing a challenge response operation. To avoid invalidating the challenge response, do NOT navigate away from the page or refresh.**
>
> **If the challenge response operation is invalidated, try restarting the process to generate a new challenge response. If that fails, contact One Identity Support for assistance.**

1. To perform a hardware factory reset, on the web management console, click **Support Kiosk**. For more information, see Support Kiosk on page 56.
2. Select **Factory Reset**. (This option is not available if you are attached to the console of a virtual machine. The options is only available for hardware.)
3. Complete the challenge/response process:
   a. In **Full Name or Email**, enter your name or email to receive the challenge question.
   b. Click **Get Challenge**.
   c. To get the challenge response, perform one of the following (see the illustration that follows).
      - Click **Copy Challenge**. The challenge is copied to the clipboard. Send that challenge to Safeguard support. Support will send back a challenge response that is good for 48 hours.
      - Screenshot the QR code and send it to Support. Support will send back a challenge response that is good for 48 hours.

        IMPORTANT: Do not reboot the machine during the challenge response process.
      - Use a QR code reader on your phone to get the challenge response.



4. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select **Factory Reset**.

Unlocking a locked cluster

In order to maintain consistency and stability, only one cluster operation can run at a time. To ensure this, SPP locks the cluster while a cluster operation is running, such as enroll, unjoin, failover, patch, reset, session module join, update IP, and audit log maintenance.

While the cluster is locked, changes to the cluster configuration are not allowed until the operation completes.

The lock notification displays as follows:

- web client: The **Appliance State** will show a red lock icon ( ).

You should never cancel the cluster lock for an SPP unjoin, failover, cluster reset, restore, patch, or IP address update. Other considerations:

- If a SPP join (enroll) is taking a long time, you may cancel it during the streaming audit data step.
- If a patch distribution is taking a long time, you may cancel it and upload the patch to the replicas directly.
- If an audit log synchronize operation is taking a long time, or you have reason to believe it will not complete due to a down appliance in the cluster, you may cancel it. Canceling this operation requires monitoring as detailed in Cancel Audit Log Maintenance from the Audit Log Maintenance page.
- If an audit log archive or purge operation is taking a long time, or you have reason to believe it will not complete due to a down appliance in the cluster, you may cancel it. Canceling this operation requires monitoring as detailed in Cancel Audit Log Maintenance from the Audit Log Maintenance page.

To unlock a locked cluster

1. Go to Cluster Management:
   - web client: Navigate to **Cluster** > **Cluster Management**.
2. Click the lock icon in the upper right corner of the warning banner.
3. In the **Unlock Cluster** confirmation dialog, enter **Unlock Cluster** and click **OK**.

   This will release the cluster lock that was placed on all of the appliances in the cluster and close the operation.

IMPORTANT: Care should be taken when unlocking a locked cluster. It should only be used when you are sure that one or more appliances in the cluster are offline and will not finish the current operation. If you force the cluster unlock, you may cause instability on an appliance, requiring a factory reset and possibly the need to rebuild the cluster. If you are unsure about the operation in progress, do NOT unlock the cluster.

Troubleshooting tips

If there is a problem with a SPP cluster, follow these guidelines:

1. Ensure that the hardware is powered on and online.
2. Check for networking problems. For more information, see Diagnosing a cluster member on page 588.

3. Check the events in the Activity Center as all cluster operations are logged. Errors and warnings may resolve on their own. If an error persists for more than 15 minutes, it probably won't resolve itself. Try restarting the appliance to see if the error or warning clears.
4. Contact One Identity Support:
    - If an appliance goes into quarantine mode, connect to the Recovery Kiosk and contact support. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.
    - Generate and collect support bundles for each appliance in the cluster and contact support. For more information, see Support bundle on page 148.

Appliance states

The following table lists the appliance states and what actions are available when the appliance is in a particular state.

Table 234: Appliance states

Appliance state and description	Actions available
EnrollingReplica (only applies to replica appliances in a cluster) A transitional state where a replica appliance is being added to a cluster and is not available for access. From this state, the appliance goes into Maintenance mode to complete the enroll operation.	Wait for operation to complete before logging in to appliance.
Initial Setup Required A virtual appliance has been deployed but cannot be used until it is in the **Online** state.	The Appliance Administrator must run Initial Setup for the virtual appliance to move to the **Online** state. For more information, see Setting up the virtual appliance on page 52.
Initializing A transitional state where the appliance is initializing to start, but is not yet available for access.	Wait for operation to complete before logging in to appliance.
Maintenance Appliance is performing maintenance tasks and is not available for access.	Wait for maintenance tasks to complete before logging in to appliance.
LeavingCluster (only applies to replica appliances in a cluster)	Wait for operation to complete before logging in to appliance.

Appliance state and description	Actions available
A transitional state where a replica appliance is being unjoined from a cluster and is not available for access. From this state, the appliance goes into Maintenance mode to complete the unjoin operation.	
Offline Appliance is not available for access.	Wait for appliance to come back online before logging in.
Offline Workflow The appliance is not communicating with the cluster but has been either automatically or manually placed in Offline Workflow Mode to run access request workflow.	Enable Offline Workflow Mode. Once online operations are resumed, the appliance is returned to Maintenance mode. For more information, see About Offline Workflow Mode on page 581.
Online The appliance is a primary and has consensus. Or the appliance is a replica and has both consensus and connectivity to the primary.	Log in to appliance. In this state, access request workflow is available from all clustered appliances that are online and able to communicate.
PatchPending (only applies to replica appliances in a cluster) Upon cluster patch, the primary appliance instructs all replicas to enter PatchPending state. The primary appliance then patches and upon completion, instructs the PatchPending replicas to install the patch one at a time.	You can log in to a replica with a PatchPending state. You can initially perform access request workflow on a replica in PatchPending state; however, during the cluster upgrade, when the majority of the cluster members have upgraded, access request worklfow migrates from the PatchPending side of the cluster to the upgraded side of the cluster. During this time, access request workflow is unavailable on any appliance still in the PatchPending state.
PrimaryNoQuorum (only applies to the primary appliance in a cluster) The primary appliance is in a Read-only mode while attempting to get the lease, but can't because the cluster does not have consensus. The appliance continues to attempt getting the lease and when it does, the appliance state goes back to Online.	If the appliance is powered on, you can log in to an appliance with a PrimaryNoQuorum state; however, it will be in a Read-only mode. In this state, access request workflow is not available from the primary appliance, but may be available from other appliances in the cluster. For example, if the primary cannot

Appliance state and description	Actions available
	communicate with the rest of the nodes in the cluster, but the rest of the nodes can communicate between themselves (ReplicaWithQuorum state), then access request workflow will be available from these replica appliances even though it is not available from the primary appliance.
Quarantine Appliance is broken or in an unknown state.	Requires manual intervention to recover. Go to the Recovery Kiosk to recover. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.
ReplicaDisconnected (applies to replica appliances in a cluster) A replica appliance is available for access; however, both of the following conditions apply: • The replica appliance cannot communicate with the primary appliance in the cluster. • The remaining nodes in the cluster that the replica appliance can communicate with do not have consensus.	You can log in to a replica with a ReplicaDisconnected state, but access request workflow is disabled. If the replica appliance cannot communicate with the other nodes in the cluster, but the remaining nodes can communicate with each other, then access request workflow will be available from those appliances even though it is not available from the appliance that cannot communicate with them.
ReplicaNoQuorum (applies to replica appliances in a cluster) A replica appliance can communicate with the primary appliance; however, the remaining nodes in the cluster do not reach consensus. Once the cluster regains consensus, the replica appliance will go into the Online state.	You can log in to a replica with a ReplicaNoQuorum state, but access request workflow is disabled. In this state, access request workflow is not available from the primary appliance, but may be available from other replicas. For example, in a cluster of five appliances, if the primary and a single replica cannot communicate with the remaining replicas in the cluster, but the other three replicas in the cluster can communicate between themselves (ReplicaWithQuorum state), then access request workflow will be available from the replicas that are online and communicating even though it is not available from the primary and replica that cannot communicate.

Appliance state and description	Actions available
ReplicaWithQuorum (applies to replica appliances in a cluster) A replica appliance cannot communicate with the primary appliance; however, the remaining nodes in the cluster have reached consensus.	You can log in to a replica with a ReplicaWithQuorum state. In this state, access request workflow is available from any clustered appliance that is online and able to communicate. Passwords and SSH keys can be requested and checked in. Scheduled tasks will not occur until after the cluster patching is complete. Manual check and change is not available. The policy may be configured such that a password or SSH key reset is required before the password or SSH key can be checked out again. If that is the case, the following can be temporarily configured prior to cluster patching and access request to allow for password or SSH key check out when a password or SSH key has not been reset. • The policy can be set to allow multiple accesses. • The policy can be set to not require a password or SSH key change at check in. • Emergency requests can be allowed so the user does not have to wait for the password or SSH key to be reset.
TransitioningToPrimary (only applies to replica appliances in a cluster) A transitional state where a replica appliance is being promoted to be the new primary and is not available for access.	Wait for operation to complete before logging in to appliance.
TransitioningToReplica (only applies to the primary appliance in a cluster.) A transitional state where a primary appliance is being demoted to a replica and is not available for access.	Wait for operation to complete before logging in to appliance.
ShuttingDown A transitional state where an appliance is shutting down and is not available for access.	Wait for appliance to come back online before logging in.

Appliance state and description	Actions available
StandaloneReadOnly State used for replicas unjoined from a cluster or a primary appliance restored from a backup. The appliance can be activated.	Log in to appliance. See Activating a read-only appliance for how to activate a Read-only appliance so you can add, delete and modify data, apply access request workflow, and so on.
Unknown Appliance is broken or in an unknown state.	Requires manual intervention to recover. Go to the Recovery Kiosk to recover. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.
HardwareSecurityModuleError The appliance can no longer access the configured Hardware Security Module for decryption. This state only occurs on startup or during the connection checks that run every 4 hours. During startup, any error to connect to the Hardware Security Module will cause the appliance to transition to this state. During a connection check, networking issues will not cause the appliance to transition to this state.	All Hardware Security Module related actions are available. This includes managing Hardware Security Module Client and Server certificates, updating the Hardware Security Module configuration, running cluster health checks, and running Hardware Security Module verifications. The appliance will transition out of this state when a valid configuration exists that allows the appliance to decrypt, and either: • The next connection check runs (every 4 hours). • A Hardware Security Module verification is run, either through a cluster member health check, or through a refresh on the Hardware Security Module external integration menu.

16

Administrator permissions

To secure control of your IT department's assets (that is, managed systems), SPP uses a role-based access control hierarchy. SPP's various permission sets restrict the amount of control each type of user has.

NOTE: It is the responsibility of a user with Authorizer Administrator permissions to grant administrator permissions to other SPP users; however, the User Administrator can grant Help Desk Administrator permissions to non-administrative users.

Administrator permissions include:

- Appliance Administrator permissions
- Asset Administrator permissions
- Auditor permissions
  - System Auditor
  - Application Auditor
- Authorizer Administrator permissions
- Help Desk Administrator permissions
- Operations Administrator permissions
- Security Policy Administrator permissions
- User Administrator permissions

Appliance Administrator permissions

The Appliance Administrator is responsible for configuring and maintaining the appliance, including the following tasks:

- Racks and stacks the appliance.
- Configures the appliance.
- (Optional) Sets up and uses the virtual appliance for initial setup, maintenance, backup, and recovery. For more information, see Using the virtual appliance and web management console on page 50.

- Troubleshoots performance, hardware, and networking.
- Creates and monitors the status of a clustered environment.
- Manages licenses, certificates, backups, and sessions settings.
- Enables and disables access request and password and SSH key management services.

Asset Administrator permissions

An Asset Administrator manages all partitions, assets, and accounts:

- Creates (or imports) assets and accounts.
- Creates partitions and profiles.
- Delegates partition ownership to users. A delegated partition owner has a subset of permissions that an Asset Administrator has. That is, the delegated partition owner is authorized to manage a specific partition and the assets and accounts assigned to that partition.
- Assigns assets to partitions.
- Manages account password rules.
- Manages ownership for assets, accounts, and partitions.

NOTE: Asset Administrators can only view the user object history for their own account.

Auditor permissions

The Auditor administrator has read-only access to all features, and has the ability to review all access request activity:

- Monitor appliance information
- Review everything
- Export object history
- Run entitlement reports

There are two additional permission types available once the Auditor role is selected that will help provide limited auditor permissions should you prefer not to use the all-encompassing Auditor role (which incorporates both permission types):

- Application Auditor
- System Auditor

On some pages, it may appear the administrator can edit data, but the change cannot be saved. A message like the following will display: `Authorization is required for this request.`

Application Auditor

Application Auditor provides read-only access to features related to the functionality of Safeguard. The Application Auditor permissions correspond with the following roles, however only read-access is allowed:

- Security Policy
- Asset

System Auditor

System Auditor provides read-only access to features related to the operation of Safeguard. The System Auditor permissions correspond with the following roles, however only read-access is allowed:

- Appliance
- Operations
- Help Desk
- User
- Global

Authorizer Administrator permissions

The Authorizer Administrator is the permissions administrator and performs the following:

- Creates (or imports) SPP users.
- Grants administrator permissions to users.
- Sets passwords, unlocks, and enables or disables both local and directory user accounts.

The Authorizer Administrator also has User Administrator and Help Desk Administrator permissions.

> IMPORTANT: Authorizer Administrators can change the permissions for their own account, which may affect their ability to grant permissions to other users. When you make changes to your own permissions, they take effect next time you log in.

Help Desk Administrator permissions

A Help Desk Administrator:

- Sets passwords for non-administrative user accounts.
- Unlocks accounts for all user accounts.

NOTE: Help Desk Administrators can only view the user object history for their own account.

Operations Administrator permissions

The Operations Administrator monitors the status of the appliance and can reboot the appliance.

On some pages, it may appear the administrator can edit data, but the change cannot be saved. A message like the following will display: `Authorization is required for this request.`

NOTE: This user can be a non-interactive user; that is, an automated script or external monitoring system.

Security Policy Administrator permissions

The Security Policy Administrator configures the security policies that govern the access rights to accounts and assets, including the requirements for checking out passwords, such as the maximum duration, if password or SSH key reasons are required, if emergency access is allowed, and so on. This user may not know any details about the assets.

This user configures time restrictions for entitlements and who can request, approve and review access requests.

- Creates account groups, asset groups, and user groups.
- Creates entitlements.
- Configures access request policies.
- Adds users or user groups to entitlements to authorize those accounts to request passwords.
- Can assign linked accounts to users for entitlement access policy governance.

On some pages, it may appear the administrator can edit data, but the change cannot be saved. A message like the following will display: `Authorization is required for this request.`

User Administrator permissions

The User Administrator:

- Creates (or imports) SPP users.
- Creates user groups.
- Grants Help Desk Administrator permissions to users.
- Sets passwords, unlocks users, and enables or disables non-administrator user accounts.
- Also has Help Desk Administrator permissions.

Considerations:

- User Administrators cannot modify administrator passwords, including their own.
- User Administrators can change the permissions for their own account, which may affect their ability to grant Help Desk Administrator permissions to other users. When you make changes to your own permissions, they take effect next time you log in.

17

Preparing systems for management

Before you add systems to SPP (Adding an asset), you must ensure they are properly configured.

Generally, to prepare an asset for SPP:

1. Create a functional account (called a "service" account in SPP) on the asset and assign it a password or an SSH key, if the platform supports SSH keys.

   NOTE: To add an asset to SPP, it must have a service account. For more information, see About service accounts on page 321.

2. Grant the service account sufficient permissions.
3. Test the service account connectivity.
4. Configure the security protocol.
5. For platforms that support SSL server certificate validation, add the server's signing authority certificate to the Trusted Certificates store in SPP. For more information, see Trusted CA Certificates on page 193.

The following topics can help you prepare your hosts for management by SPP:

Preparing ACF - Mainframe systems

Preparing Amazon Web Services platforms

Preparing Cisco devices

Preparing Dell iDRAC devices

Preparing VMware ESXi hosts

Preparing Fortinet FortiOS devices

Preparing F5 Big-IP devices

Preparing HP iLO servers

Preparing HP iLO MP (Management Processors)

Preparing IBM i (AS/400) systems

Preparing JunOS Juniper Networks systems

Preparing MongoDB

Preparing MySQL servers

Preparing Oracle databases

Preparing PAN-OS (Palo Alto) networks
Preparing PostgreSQL
Preparing RACF mainframe systems
Preparing SAP HANA
Preparing SAP Netweaver Application Servers
Preparing Safeguard for Privileged Sessions for credential management
Preparing Sybase (Adaptive Server Enterprise) servers
Preparing SonicOS devices
Preparing SonicWALL SMA or CMS appliances
Preparing SQL Servers
Preparing Top Secret mainframe systems
Preparing Unix-based systems
Preparing Windows systems
Preparing WinRM systems
Preparing Windows SSH systems
VMware vCenter Server
Minimum required permissions for Windows assets

SPP supports a variety of platforms. For more information, see Supported platforms on page 33.

Preparing ACF - Mainframe systems

This applies to both ACF2 - Mainframe and ACF2 - Mainframe LDAP platforms.

To prepare IBM ACF-mainframe systems for SPP

1. Create a service account on the asset and assign it a password. The service account must have the `SECURITY` attribute enabled for ACF2 ChangePassword to work properly.
2. Grant the service account the privileges required to use the `ALTERUSER` command on other profiles.
3. If not already installed, install a telnet server on the z/OS system. If required, secure telnet with SSL.

   NOTE: Please refer to your IBM z/OS system documentation for details on installing and configuring the telnet server (and SSL).
4. Test the telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an z/OS system.

5. In SPP, create the asset and accounts for the z/OS system using password authentication.

About certificate support for the telnet protocol

SPP automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, SPP does not support client certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, SPP cannot support that configuration.

Preparing Amazon Web Services platforms

SPP supports Amazon Web Services (AWS), a secure cloud services platform.

When adding an Amazon Web Services asset, the **Network Address** must contain the AWS Account ID or Alias.

To prepare Amazon Web Services platforms for SPP

1. In SPP:
    a. Ensure the latest Amazon's certificate and AWS certificate's root certificate authority (CA) are in the Trusted Certificates store in SPP.
    b. Configure an Identity and Access Management (IAM) user to use as a service account.
    c. Assign the IAM service account to the AdministratorAccess security policy.
2. In Amazon:
    a. Create an access key for the IAM service account. Amazon creates a pair of data items called a Secret Key and a public Access Key ID. Take a note of both the Access Key ID and Secret Key. You will need them when you add the Amazon Web Services asset to SPP.

Preparing Cisco devices

There are 4 Cisco platforms supported in SPP:

- Cisco ISE CLI platform: SPP uses a local service account to manage accounts on the ISE CLI platform using SSH.
- Cisco IOS/ASA platform: Cisco IOS/ASA platforms can be configured in the following ways to manage local accounts using SSH:

    - SPP uses a local service account to manage accounts on the Cisco device.
    - If the Cisco device is configured (using AAA) to authenticate and authorize login requests to a Cisco ISE server that will be managed by SPP, then you can use a directory account in the Cisco ISE directory asset to manage the Cisco device.
    - If the Cisco device is configured (using AAA) to authenticate and authorize login requests to a Cisco ISE server that is integrated with an Active Directory domain that will be managed by SPP, then you can use a directory account in the Active Directory asset to manage accounts on the Cisco device.
    - If the service account is not configured with privilege level 15, then the enable password for privilege level 15 will be required when creating the asset.
- Cisco ISE platform: Cisco ISE is managed as a directory asset in SPP. It uses REST and TACACS+ to manage local accounts. It supports account discovery and password management. It does not support directory synchronization, asset discovery, or service discovery.
- Cisco NX-OS platform: In order to perform all required operations on users, the service account used requires at least network-admin privileges.

Cisco ISE CLI platform

SPP manages local accounts on the ISE CLI platform using SSH.

To manage local accounts on the Cisco ISE CLI platform

1. Enable and configure the SSH server to allow the service account to log in remotely.
2. Create a service account (with the admin role) on the asset and assign it a password.

Cisco IOS/ASA platform

Safeguard for Privileged Passwords supports both Cisco Private Internet eXchange (PIX) firewall security appliances and PIX Internetwork Operating System (IOS) routers and switches. Cisco PIX and Cisco IOS use the SSH protocol to connect to the Safeguard for Privileged Passwords Appliance. Safeguard for Privileged Passwords supports both SSH version 1 and version 2.

The following applies:

- SPP uses SSH to manage accounts on the Cisco platform. The SSH server must be enabled and configured to allow the service account to log in remotely.
- SPP manages accounts found in the startup configuration file, not in the running configuration file.
- The selected service accounts must have sufficient privileges to update configuration. If the user does not have sufficient privileges on login, then the **Privilege Level Password** (that is, the system enable password) must be configured for the asset in SPP.

Local configuration

The following information is for preparing a Cisco device using a local service account.

To prepare a Cisco device for SPP using a local service account

1. Create a service account on the asset and assign it a password.
2. Enable and configure the SSH server to allow the service account to log in remotely.
3. If required, configure the **Privilege Level Password** (that is, the system enable password).
4. Add the Cisco device to SPP using password authentication.

Directory Configuration using Cisco ISE Directory

IMPORTANT: For full details on how to configure your Cisco ISE server and ISE policy, refer to your system documentation.

If the Cisco device is configured (using AAA) to authenticate and authorize login requests to a Cisco ISE server that will be managed by SPP, then you can use a directory account in the Cisco ISE directory asset to manage the Cisco device.

Alternatively, if the Cisco ISE server is integrated with an Active Directory domain that will be managed by SPP, then you can use a service account from the integrated AD directory to manage the asset. In this scenario, you only need to create the AD asset; you do not need to create a Cisco ISE server asset in SPP.

To prepare the Cisco ISE server to manage the Cisco IOS/ASA asset using a directory account

1. Create a service account in the Cisco ISE server:
   a. To authenticate to the Cisco ISE server:
      i. Create a local **Network Access** user.
      ii. Set **PasswordType** to **Internal Users**. This authenticates the user locally.
      iii. Assign a password for the user.
   b. To authenticate to Active Directory:
      i. Create an External Identity Source for the domain that will be managed by SPP.
      ii. Join the Cisco ISE server to the domain, and import any AD groups that you wish to use in the ISE policy.
      iii. Create a **Network Access** user with the username matching the AD username.
      iv. Set **PasswordType** to `<domainname>`. Do NOT assign the user a password (the password is authenticated to AD).
2. Configure a **Network Device** to permit TACACS+ access from the Cisco device to the Cisco ISE server. Configure the TACACS+ shared secret to match the shared secret you have configured using AAA on the Cisco device.
3. Configure a **Device Admin Policy** to grant shell login for the selected **Network Access** user to the selected **Network Device**. The policy can be configured in ISE based on many different session, user, or group settings.

NOTE: For example:

1. Create an **Identity Group** to represent all the **Network Access** users to be managed by SPP.
2. Import an AD group that represents all the AD users that will be used by SPP to access the network device.
3. Create a policy to grant shell login to all members of these groups.

   A CheckPassword request or Safeguard for Privileged Sessions session from SPP will then fail for any **Network Access** user not in either group.

To prepare the Cisco IOS/ASA asset to be managed by an ISE account

1. Enable and configure the SSH server to allow the service account to log in remotely.
2. Configure AAA to use TACACS+ to authorize login requests to the Cisco ISE server for directory users, using the shared secret configured for this network device in the Cisco ISE server.

   NOTE: Refer to your system documentation for details of how to configure AAA.
3. Test that the selected Cisco ISE **Network Access** user can login to the Cisco device. This can be tested by logging in from the command line using SSH.
4. As appropriate, add the selected service account to the Cisco ISE or AD directory asset in SPP.
5. If required, configure the **Privilege Level Password** for the Cisco IOS asset.
6. Add the Cisco device to SPP using directory authentication.
7. If you need to configure the asset for Safeguard for Privileged Sessions session access, check that the server-side SSH algorithms configured in Safeguard for Privileged Sessions include algorithms supported by the Cisco device.

Cisco ISE platform

Cisco ISE is managed as a directory asset in SPP. It supports account discovery and password management. It does not support directory synchronization, asset discovery, or service discovery.

A Cisco ISE directory user can be used:

- as a service account to manage a Cisco IOS/ASA asset that is configured to authenticate login requests to the Cisco ISE server.
- to run a Safeguard for Privileged Sessions managed SSH session on a Cisco IOS/ASA asset that is configured to authenticate login requests to the Cisco ISE server.

SPP manages **Network Access** (internal) users in the Cisco ISE server (it does NOT manage local Admin Users). The **Network Access** users are directory accounts that can be used to login to other network devices (e.g. Cisco IOS assets). The managed network devices must be configured to use AAA to authenticate and authorize requests to the Cisco ISE server (For more information, see your system documentation).

The service account on the ISE platform must be a **Network Access** user with administrative privileges.

Preparing Cisco ISE

1. SPP uses the ISE REST API (ERS) to manage passwords in Cisco ISE. This is disabled by default, so must be enabled for read/write access in the **System Settings** before Cisco ISE can be configured.
2. Safeguard uses the TACACS+ protocol to verify passwords in Cisco ISE. This is disabled by default, so must be configured by enabling the **Device Admin Service** in the Cisco ISE server's **Global Settings**.
3. Create a **Network Access** user (set **PasswordType** to **Internal Users**) and assign it a password. Do NOT configure an **Enable Password**.
4. Assign Administrative access to the new user by creating an **Admin User**, and select the new user from the list of existing Network Access users instead of creating a new user.
5. Add the selected Admin User to either of the following Admin groups:
   - **Super Admin**
   - **ERS Admin** and **Elevated System Admin**
6. Configure a **Network Device** for your SPP cluster.
   a. Add the IP addresses of appliances in your SPP cluster.
   b. Configure the TACACS+ secret for the cluster to use.

   > NOTE: This must match the TACACS+ shared secret configured on the Cisco IOS/ASA network devices that you wish to manage using directory users in this asset.
7. Configure a **Device Admin Policy Set** that includes the following:
   - Grant TACACS+ access to the **Network Device** configured for your SPP cluster.
   - Allow all TACACS+ protocols.
   - Grant shell access to the **Network Access** users that you wish to manage using SPP. The policy can be configured in ISE based on many different session, user or group settings.

   > NOTE: For example:
   >
   > 1. Create an **Identity Group** to represent all the **Network Access** users to be managed by SPP.
   > 2. Create a policy to grant shell login to all members of this group.
   >
   > A CheckPassword request or Safeguard for Privileged Sessions session from SPP will then fail for any **Network Access** user not in either group.
8. Configure port 49 for TACACS+.

Cisco NX-OS platform

SPP manages local accounts on the Cisco NX-OS platform using NX-API.

To manage local accounts on the Cisco NX-OS platform

1. Enable the NX-API feature to allow the service account to log in remotely and execute commands over NX-API.
2. Create a service account (with the network-admin role) on the asset and assign it a password.

Preparing Dell iDRAC devices

SPPsupports the Dell Remote Access Controller that is integrated with Dell PowerEdge servers. SPP uses the SSH protocol to connect to iDRAC devices.

To prepare an iDRAC device for SPP

1. Use iDRAC to create a service account with administrator privileges and assign it a password.

   The service account must have login privileges and must be able to configure users.
2. Verify that SSH is enabled in the iDRAC Network settings.
3. In SPP, create the asset and accounts for the iDRAC device using password authentication. Accounts can also be discovered.

Preparing VMware ESXi hosts

SPP supports VMware ESXi hosts.

IMPORTANT: SPP can only manage local users on a VMware host.

To prepare a VMware ESXi host for SPP

1. Use an existing account or create a new account as the service account on the asset and assign it a password.

   The default administrator account is suitable.
2. Grant the service account the privileges required to set user passwords using the web management API.
3. When adding a VMware ESXi host to SPP:
   a. Specify the network address.
   b. Specify port 443 as the HTTPS port.

Preparing Fortinet FortiOS devices

SPP supports Fortinet Internet appliances. SPP uses the SSH protocol to connect to Fortinet devices.

To prepare a Fortinet FortiOS device for SPP

1. Create the service account as a local user on the managed system and assign it a password.
2. Add the service account to the Fortinet Administrators group. This allows the service account to access the device with SSH to manage users.

   IMPORTANT: SPP can only manage passwords for users that are members of the Fortinet Administrators group.
3. Enable and configure the SSH server to allow the service account to log in remotely.
4. Add the Fortinet device to SPP using password authentication.

Preparing F5 Big-IP devices

SPPsupports F5 Big-IP devices. SPP uses the SSH protocol to connect to F5 Big-IP devices.

To prepare an F5 Big-IP device for SPP

1. Create the service account as a local user on the F5 Big-IP managed system and assign it a password. Assign that service account the Administrator Role on all partitions. This allows the service account to manage users.
2. Enable console access by setting **Terminal Access** to either **Advanced** or **tmsh**, which will allow the service account to log in remotely via SSH.
3. Add the F5 Big-IP device to SPP using password or SSH key authentication.

Preparing HP iLO servers

In SPP, the **HP iLO** operating system is an HP Integrated Lights-Out (iLO) HP Proliant server. SPP connects to HP iLO systems using SSH. Password check and change is supported.

To prepare an HP iLO server for SPP

1. Create a service account with the Administrate User Accounts privilege and assign it a password.

   The service account must have login privileges and must be able to configure users.
2. Verify that SSH is enabled.

3. In SPP, create the asset and accounts for the HP iLO server using password authentication. Accounts can also be discovered.

Preparing HP iLO MP (Management Processors)

In SPP the **HP iLO MP** operating system is an HP Integrity Integrated Lights-Out (iLO) Management Processor. SPP connects to HP iLO MP systems using SSH.

To prepare an HP iLO Management Processor for SPP

1. Create a service account with the Administer User Accounts privilege and assign it a password.
2. Verify that SSH is enabled.
3. In SPP, create the asset and accounts for the HP iLO MP asset type using password authentication. Accounts can also be discovered.

Preparing IBM i (AS/400) systems

SPP supports IBM i systems (formerly known as AS/400).

To prepare IBM i systems for SPP

1. Create a service account on the asset and assign it a password.
2. Grant the service account the privileges required to use the `chgusrprf` command on other profiles.
3. If not already installed, install a telnet server on the IBM iSeries (AS/400) system. If required, secure telnet with SSL.

   NOTE: Please refer to your IBM iSeries (AS/400) system documentation for details on installing and configuring the telnet server (and SSL). See the IBM Knowledge Center.

4. Test the telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an IBM iSeries system.
5. In SPP, create the asset and accounts for the IBM iSeries (AS/400) system using password authentication.

About certificate support for the telnet protocol

SPP automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, SPP does not support client

certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, SPP cannot support that configuration.

Preparing JunOS Juniper Networks systems

SPPuses the Juniper Networks JunOS operating system to manage Juniper Networks routers and switches. SPP connects to JunOS systems using SSH.

> **CAUTION: If you get the message: `Shared configuration database modified`, the global configuration is currently being edited. The edits must be committed or discarded so Safeguard can enter configure private mode. To resolve the problem, log in to the box interactively with SSH, run `configure`, and then run `status` to review the sessions currently editing the global configuration. Run `rollback` to discard any edits or `commit` to commit the changes.**

To prepare a Juniper Networks JunOS system for SPP

1. Create a service account that is a member of the super-user login class and assign it a password.
2. Verify that SSH is enabled.
3. In SPP, create the asset and accounts for the Juniper Networks JunOS asset type using password authentication.

Preparing MongoDB

SPPmakes an SSL connection to MongoDB using a TCP port and Bind IP address defined in the `mongodb.conf` file. You must enter this port number when adding a MongoDB asset to SPP.

To configure MongoDB for SPP

1. Create a service account and assign it a password.

   > NOTE: The service account must have permissions for remote connections and permissions to change passwords. Consult your MongoDB Security Guide for the appropriate settings for your organization.

2. Verify that you can log in with the service account.
3. In SPP, create the asset and accounts for the MongoDB asset type using password authentication. You must specify the **Database instance name** and the **Port** used by the database instance.

NOTE: When you create an account of Dialog User or Communication Data type, SPP allows you to set the account password or reset the password. Use the **Reset Password** option to reset the password for this account. If you use the **Set Password** option and enter the same password used in MongoDB, the password check in SPP will fail.

Preparing MySQL servers

To prepare a MySQL server for SPP, refer to the documentation for your MySQL server for information about how to setup and secure encryption.

To enable SSL server certificate validation, add the server's signing authority certificate to the Trusted Certificates store in SPP. For more information, see Trusted CA Certificates on page 193.

For more information about how SPP database servers use SSL, see How do SPP database servers use SSL on page 669.

SQL accounts supported

Safeguard can support MySQL accounts that have been created with the format `<username>` or `<username>@< range of IP addresses>`. The permitted range of IP addresses must include the IP address of the Safeguard appliance. The % character can be used as a wildcard.

Examples:

- Sam : Permit Sam to log in from any host (default)
- Sam@%: Permit Sam to log in from any host
- Sam@10.1.%: Permit Sam to log in from any IP address in 10.1.xx

Preparing Oracle databases

To prepare an Oracle database for SPP, refer to the documentation for your Oracle database for information about how to set up and secure encryption.

To enable SSL server certificate validation, when configuring the SSL-enabled service on the Oracle server, ensure that the following security setting is configured:

`SSL_SERVER_CERT_DN="CN=<address>"`, where *<address>* matches the Network Address of the asset in SPP.

Preparing PAN-OS (Palo Alto) networks

In SPP the PAN-OS operating system is used by Palo Alto Networks appliances. SPP connects to PAN-OS systems using SSH.

To prepare a Palo Alto Networks system for SPP

1. Create a service account that is a Device Administrator and assign it the Superuser role and a password.
2. Verify that SSH is enabled.
3. In SPP, create the asset and accounts for the Palo Alto Networks asset type using password authentication.

Preparing PostgreSQL

SPP makes an SSL connection to PostgreSQL using a TCP port defined in the `postgresql.conf` file. You must enter this port number when adding a PostgreSQL asset to SPP.

To configure PostgreSQL for SPP

1. Create a service account and assign it a password.

   NOTE: The service account must have permissions for remote connections, modify log_statements (if you want to enable the **Hide Alter User command from verbose log_statement logging** option), and permissions to change passwords.

   Alter User commands can be excluded from the PostgreSQL server logs during SPP password changes. The option to hide Alter User commands is enabled by default for new PostgreSQL assets starting with SPP 7.1 with verbose log_statement logging. Customers upgrading to 7.1 that want to enable the option will need to reconfigure any existing PostgreSQL assets with verbose log_statement logging to have a service account with superuser permissions and enable the option.

   Consult your PostgreSQL Security Guide for the appropriate settings for your organization.
2. Verify that you can log in with the service account.
3. In SPP, create the asset and accounts for the PostgreSQL asset type using password authentication. You must specify the **Database instance name** and the **Port** used by the database instance. Accounts can also be discovered.

   NOTE: When you create an account of Dialog User or Communication Data type, SPP allows you to set the account password or reset the password. Use the **Reset Password** option to reset the password for this account. If you use the **Set Password** option and enter the same password used in PostgreSQL, the password check in SPP will fail.

Preparing RACF mainframe systems

This applies to both RACF mainframe and RACF mainframe LDAP platforms.

To prepare IBM RACF mainframe systems for SPP

1. Create a service account on the asset and assign it a password.
2. Grant the service account the privileges required to use the `ALTERUSER` command on other profiles.
3. If not already installed, install a telnet server on the z/OS system. If required, secure telnet with SSL.

   NOTE: Please refer to your IBM z/OS system documentation for details on installing and configuring the telnet server (and SSL).
4. Test the telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an z/OS system.
5. In SPP, create the asset and accounts for the z/OS system using password authentication.

About certificate support for the telnet protocol

SPP automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, SPP does not support client certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, SPP cannot support that configuration.

Preparing SAP HANA

SPPmakes an SSL connection to SAP HANA using a TCP port between 30015 and 39915, depending on the SAP system number (also known as the "instance number"). For more information, see Safeguard ports on page 676.

To configure SAP HANA for SPP

1. Create a service account and assign it a password.

   This service account must have permissions for remote connections and permissions to change passwords. Consult your SAP security guide for the appropriate settings for your organization.
2. Verify that you can log in with the service account.

   In SAP, when you create a new account of Dialog User or Communication Data type, you will be prompted to set a new password.

3. In SPP, create the asset and accounts for the SAP Hana asset type using password authentication. You must specify the **SAP HANA Service Name** as well as the **Port** used by the SAP instance.

   When you create an account of Dialog User or Communication Data type, SPP allows you to set the account password or reset the password. Use the **Reset Password** option to reset the password for this account. If you use the **Set Password** option and enter the same password used in SAP, the password check in SPP will fail.

Preparing SAP Netweaver Application Servers

SPPmakes an SSL connection to the SAP Application Server using a TCP port between 3300 and 3399, depending on the SAP system number (also known as the instance number). You can have multiple instances of SAP running on a server, each using a different network port in the range of 3300-3399. The last two digits of the port are called the system number (or instance number). For more information, see Safeguard ports on page 676.

When you assign a password to the account, the account is not usable until you log in and change the password from the admin-assigned value.

If a privileged user for the asset is of System or Communication User Type, assign RFC authorization for the RFCPING function module for that user. This allows the user to execute its functions remotely, such as changing the password.

To configure a SAP Netweaver Application Server for SPP

1. Create a service account and assign it a password.

   This service account must have permissions for remote connections and permissions to change passwords. Settings may include:

   - Cross-application Authorization Objects set to Authorization Check for RCF Access
   - Basis: Administration set to User Master Maintenance: User Groups including Change and Lock

   The S_A.SYSTEM authorization profile will work, but may have more permissions than are necessary.

   Consult your SAP security guide for the appropriate settings for your organization.

2. Verify that you can log in with the service account.

   In SAP, when you create a new account of System or Communication User Type, you will be prompted to set a new password.

3. In SPP, create the asset and accounts for the SAP Hana asset type using password authentication. You must specify the **SAP HANA Service Name** as well as the **Port** used by the SAP instance.

When you create an account of System or Communication User Type, Safeguard allows you to set the account password or reset the password. Use the **Reset Password** option to reset the password for this account. If you use the **Set Password** option and enter the same password used in SAP, the password check in Safeguard will fail.

Preparing Safeguard for Privileged Sessions for credential management

SPP supports managing Safeguard for Privileged Sessions credentials.

Before configuring Safeguard for Privileged Sessions to allow for credential management, the following should be considered:

- The `root` and local `admin` accounts will automatically be added to account discovery results. If a local `root` account exists, it will be ignored and unmanageable.
- The `root` account name will always be considered the Safeguard for Privileged Sessions SSH console account. It can allow both SSH Key and password requests. All other local accounts can only allow password requests.
- Accounts can be manually added to SPP or managed through account discovery.
- SSafeguard for Privileged Sessions provides configurable brute-force attack protection. You may need to adjust the settings to avoid blacklisting a user or the SPP IP address.

To prepare Safeguard for Privileged Sessions for SPP credential management

IMPORTANT: For Safeguard for Privileged Sessions assets, if you're using both REST and SSH as part of your management protocol they will need to be hosted on the same IP.

If using a Safeguard for Privileged Sessions cluster, ensure the clustered nodes have the Managed Host role enabled.

1. Use the local `admin` account as the service account, or another local Safeguard for Privileged Sessions user with admin privileges. Consult the Safeguard for Privileged Sessions documentation for the appropriate settings for your organization.
2. Verify that you can test the connection using the service account.
3. In SPP, create the asset for the Safeguard for Privileged Sessions platform using password authentication.
4. After creating the SPP accounts (either manually or through account discovery), you must **Set Password** (for more information, see Checking, changing, or setting an account password).

Preparing Sybase (Adaptive Server Enterprise) servers

To prepare a Sybase ASE (Adaptive Server Enterprise) server for SPP, refer to the documentation for your Sybase ASE server for information about how to setup and secure encryption. Make sure the service account you use has the sso_role assigned.

To enable SSL server certificate validation, add the server's signing authority certificate to the Trusted Certificates store in SPP. For more information, see Trusted CA Certificates on page 193.

For more information about how SPP database servers use SSL, see How do SPP database servers use SSL on page 669.

Preparing SonicOS devices

SPPsupports SonicOS Internet appliances. SPP uses the SSH protocol to connect to SonicOS devices.

To prepare a SonicOS device for SPP

1. Create the service account as a local user on the managed system and assign it a password.
2. Add the service account to the SonicWALL Administrators group. This allows the service account to access the device with SSH to manage users.

   > IMPORTANT: SPP can only manage passwords for users that are members of the SonicWALL Administrators group.

3. Enable and configure the SSH server to allow the service account to log in remotely.
4. Add the SonicOS device to SPP using password authentication.

Preparing SonicWALL SMA or CMS appliances

Here are some important notes about configuring a SonicWALL SMA or CMS appliance for SPP:

1. Use the local admin account as the service account.
2. SPP can only manage the admin account; it cannot manage other local accounts or accounts from external providers.

Preparing SQL Servers

To prepare a MicrosoftSQL Server for SPP, refer to the documentation for your SQL server for information about how to set up and secure encryption.

To enable SSL server certificate validation, add the server's signing authority certificate to the Trusted Certificates store in SPP. For more information, see Trusted CA Certificates on page 193.

For more information about how SPP database servers use SSL, see How do SPP database servers use SSL on page 669.

To configure a SQL Server for SPP (with an authentication type of Local System Account)

NOTE: To manage a Microsoft SQL server asset with the authentication type of **Local System Account**, you need a local Windows account that is a **Security Admin** in SQL. In order to use this authentication type, you must add a Windows asset and an SQL Server asset to SPP.

1. Log in to the SPP client as an Asset Administrator.
2. Navigate to **Asset Management** > **Assets**.
3. Add a Windows asset that matches the OS of the server that is hosting the SQL database.
   a. On the **Connection** tab:
      - **Authentication Type**: Set to **Password**.
      - **Service Account**: Set to a local user that is a member of the Administrator's group.
   b. Add other accounts as needed.

   Save the asset.
4. Add an SQL Server asset.
   a. On the Connection tab:
      - **Authentication Type**: Set to **Local System Account**.
      - **Service Account**: Click **Select Account** and select a local system account from the list.

        The accounts available for selection are Windows accounts that are linked to the Windows asset you added in Step 3.
      - Run **Test Connection** and verify the connection works.

   Save the asset.

To configure a SQL Server for SPP (with an authentication type of Directory Account)

NOTE: To manage a Microsoft SQL asset with the authentication type of **Directory Account**, you need a domain account that is a **Security Admin** in SQL. In order to use

this authentication type, you must add a directory and directory users to SPP.

1. Add a directory and directory users.
   a. Log in as an Asset Administrator.
   b. Navigate to **Asset Management** > **Assets** to add a directory for your domain.
   c. Once added, select the domain and open the **Accounts** tab to add domain user accounts. For more information, see Adding an account to an asset on page 338.
2. Add an SQL Server asset and account information.
   a. Log in to the SPP client as an Asset Administrator.
   b. From **Asset Management** > **Assets**, add an SQL Server asset.
   c. On the **Connection** tab, complete the following:
      - **Authentication Type**: Set to **Directory Account**.
      - **Service Account**: Click **Select Account** and select a domain user account from the list.

        The accounts available for selection are domain user accounts that are linked to the directory you added in Step 1.
      - Run **Test Connection** and verify the connection works.
3. Save the asset.

To configure a SQL Server for SPP (with an authentication type of Password)

NOTE: To manage a Microsoft SQL server asset with the authentication type of **Password**, you need a local database account that is a **Security Admin** in SQL.

1. Log in to the SPP client as an Asset Administrator.
2. Navigate to **Asset Management** > **Assets**.
3. Add an SQL Server asset.
   a. On the Connection tab:
      - **Authentication Type**: Set to **Password**.
      - **Account Name**: Enter the account name.
      - Run **Test Connection** and verify the connection works.
4. Save the asset.

Preparing Top Secret mainframe systems

SPP can manage authorized Top Secret users who have a valid accessor ID (ACID) with the facility TSO who can log on to the TSO interface.

This applies to both Top Secret mainframe and Top Secret mainframe LDAP platforms.

To prepare CA Top Secret mainframe systems for SPP

1. Create a service account on the asset, assign it a password, and grant it the 'TSO' facility.
2. Grant the service account the following authority for ACIDs within its scope:
   a. Permission to list security record information for an ACID.
   b. MISC1(SUSPEND) authority, to remove the PSUSPEND attribute from ACIDs.
   c. Either ACID(MAINTAIN) or MISC8(PWMAINT) authority, to update the password of another ACID.
3. If not already installed, install a telnet server on the z/OS system. If required, secure telnet with SSL.

   NOTE: Please refer to your IBM z/OS system documentation for details on installing and configuring the telnet server (and SSL).
4. Test the telnet server using a Windows-based 3270 emulator or on Linux, use the telnet-ssl or x3270 programs to test SSL and non-SSL connections to an z/OS system.
5. In SPP, create the asset and accounts for the z/OS system using password authentication.

About certificate support for the telnet protocol

SPP automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, SPP does not support client certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, SPP cannot support that configuration.

Preparing Unix-based systems

SPP uses the SSH protocol to connect to Unix-based systems.

To prepare Unix-based systems (AIX, HP-UX, Linux, Macintosh OS X, Solaris, and FreeBSD platforms)

1. Create a service account on the asset with sufficient permissions.

   You need to at least configure a password or SSH key for the service account. If you want to use an SSH key generated and configured by SPP, then you also need to make sure the service account's home directory exists.
2. Ensure that the service account can run the following list of commands with root privileges non-interactively; that is, without prompting for a password.

   For example, on a Linux system add the following line in the sudoers file:

   ```
   <SerAcctName> ALL=(root) NOPASSWD: /usr/bin/passwd
   ```

   The commands a service account must run with root privileges non-interactively are:

Linux and most Unix-based systems:

- egrep
- grep
- modprpw (hpux only)
- passwd

> NOTE: Additional sudo commands may be required for Unix-based systems. For example, see SSH Key for a list of commands required for configuring SSH authentication keys on a managed system.

AIX:

- chuser
- sed
- grep
- passwd
- pwdadm

Mac OS X

- dscacheutil
- dscl
- passwd

3. Enable and configure the SSH server to allow the service account to log in remotely. For example, on a Mac, enable **Remote Login** for the service account.

> NOTE: Different versions of Linux and Unix may require slightly different parameters for SSH configuration. Consult a Linux/Unix system administrator or the system documentation for assistance.

Preparing Windows systems

SPP supports Windows systems. For more information, see How to: Configure Windows Assets in Safeguard.

> NOTE: Microsoft has started hardening DCOM servers which may change your configuration decisions. For more information, see https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26414 and https://support.microsoft.com/en-us/topic/kb5004442-manage-changes-for-windows-dcom-server-security-feature-bypass-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c.

To prepare Windows systems for SPP

1. Create a service account on the asset and assign it a password:
   - **Directory Configuration**

     If the Windows system is joined to a domain that will be managed in SPP, you can use a directory account, such as a Microsoft Active Directory account to manage the asset. Enable the **Password Never Expires** option; once you add the asset to SPP, you can have the service account password auto-managed to keep it secure.

     -OR-
   - **Local Configuration**

     If the Windows system is not joined to a domain, then use a local service account that has been granted sufficient permissions.
2. Grant the service account sufficient permissions to change account permissions to allow changing account passwords. For more information, see Minimum required permissions for Windows assets on page 633.
3. Configure the system's firewall to allow the following predefined incoming rules:
   - Windows Management Instrumentation (DCOM-In)
   - Windows Management Instrumentation (WMI-In)
   - NetLogon Service (NP-In)

   These rules allow incoming traffic on TCP port 135 and TCP SMB 445, respectively.
4. Ensure the following ports are accessible:
   - Port 389 is LDAP for connections. LDAP port 389 connections are used for Active Directory Asset Discovery and Directory Account Discovery.
   - Port 445 SMB is used to perform password check and changes.
   - In some cases, RPC ephemeral ports are required to be accessible for SPP to perform Service Discovery on the Windows platform (for example, Windows Server 2019 requires the ports, however Windows Server 2012 does not). For more information, see Service overview and network port requirements for Windows.
5. Change the local security policy:

   Before SPP can reset local account passwords on Windows systems, using a service account that is a non-built-in administrator, you must change the local security policy to disable the User Account Control (UAC) Admin Approval Mode (**Run all administrators in Admin Approval Mode**) option. For more information, see Change password or SSH key fails on page 638.

For additional information on ports, see Safeguard ports.

Preparing WinRM systems

Safeguard for Privileged Passwords supports Windows Remote Management (WinRM) systems.

To prepare Windows Remote Management (WinRM) systems for SPP

1. The initial configuration requirements for WinRM depend on whether or not you are using SSL.
   - For SSL (this is when **USE SSL Encryption** and **Verify SSL Certificate** are enabled for the asset):
     a. You need to manually add a CA signed certificate to the asset:

     > IMPORTANT: You will need to upload the CA certificate to Safeguard.
     >
     > On the asset, the certificate should be installed in the `LocalMachine\My store` and the CA should be in the `LocalMachine\TrustedRoots` store. If you use an intermediate that should be in the `LocalMachine\Intermediate` store.
     >
     > Ensure the following requirements are met for the certificate:
     >
     > - CN must match the hostname of the asset.
     > - CRL must be present and resolvable.
     > - Server Authentication enhanced key usage is required.

     i. The HTTPS listener needs to be registered in WinRM using the following command: `winrm create winrm/config/Listener?Address=*+transport=HTTPS '@{Hostname="<hostname>";CertificateThumbprint="<thumbprint>"}'`

     ii. Use the following command to set the certificate: `winrm set winrm/config/service '@{CertificateThumbprint="<TUMBPRINT"}'`

     iii. Open port 5986 in the firewall.

     iv. Restart the Windows Remoting service.
   - For non-SSL:
     a. On the asset, run the following command: `Enable-PSRemoting -Force`.
2. Create a service account on the asset and assign it a password:
   - **Directory Configuration**

     If the Windows system is joined to a domain that will be managed in SPP, you can use a directory account, such as a Microsoft Active Directory account to manage the asset. Enable the **Password Never Expires** option; once you add the asset to SPP, you can have the service account password auto-managed to keep it secure.

     -OR-

- **Local Configuration**

  If the Windows system is not joined to a domain, then use a local service account that has been granted sufficient permissions.

3. Grant the service account sufficient permissions to change account permissions to allow changing account passwords. For more information, see Minimum required permissions for Windows assets on page 633.

Preparing Windows SSH systems

Safeguard for Privileged Passwords supports Windows SSH systems. Windows SSH uses port 22 on the platform.

SPP requires that `C:\Windows\System32\cmd.exe` be configured as the default shell for SSH (for more information, see OpenSSH Server configuration for Windows Server and Windows).

OpenSSH on Windows 8

The OpenSSH port on Windows 8 has server-side limitations on command execution. Password operations may appear to run more slowly because commands do not return until the timeout expires, even if the command has already completed on the server. You may need to tune the Connection Timeout (CommandTimeout) when running TestConnection, ChangePassword, and CheckPassword in order to allow these password operations enough time to run while still allowing enough time to avoid timeouts for other conditions specific to your network.

To prepare Windows SSH systems for Safeguard for Privileged Passwords

1. Ensure the SSH server service is running.
2. Create a service account on the asset and assign it a password:
   - **Directory Configuration**

     If the Windows SSH system is joined to a domain that will be managed in Safeguard for Privileged Passwords, you can use a directory account, such as a Microsoft Active Directory account to manage the asset. Enable the **Password Never Expires** option; once you add the asset to Safeguard for Privileged Passwords, you can have the service account password auto-managed to keep it secure.

     -OR-

   - **Local Configuration**

     If the Windows SSH system is not joined to a domain, then use a local service account that has been granted sufficient permissions.

     > IMPORTANT: A local account does not have the access necessary to discover services running as domain accounts, so if a local account is used, SPP will

only discover and update services running as local accounts, and domain account dependencies will not be updated.

3. Ensure the service account is added to the local Administrator's group to allow change password permissions. For more information, see Minimum required permissions for Windows assets on page 633.

VMware vCenter Server

SPP manages single sign-on (SSO) accounts on the vCenter Server platform.

To manage single sign-on accounts on the VMware vCenter Server platform

1. Enable SSH access to the vCenter appliance.
2. Use the SSO administrator account as the service account when creating the asset in Safeguard.

   NOTE: If the administrator account is managed by Safeguard, then Safeguard will also attempt to synchronize

   the local root account with the SSO administrator account.

3. When creating the managed account in Safeguard, you must use the fully qualified name of the SSO account. The default fully qualified name is `<account>@vsphere.local`.

SPP supports asset discovery for the vCenter Server platform.

To discover the virtual machines in Vsphere, ensure that the service account has HTTPS access to the vCenter Server.

Minimum required permissions for Windows assets

The following minimum permissions are required for Windows assets to perform directory password management and sessions management tasks using Windows Management Instrumentation (WMI).

NOTE: Microsoft has started hardening DCOM servers which may change your configuration decisions. For more information, see https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-26414 and https://support.microsoft.com/en-us/topic/kb5004442-manage-changes-for-windows-dcom-server-security-feature-bypass-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c.

Asset password management

Using a local account or domain account:

- (Only applies to Windows Desktop and Windows Server) Test connection, Check connection, Password check, and Account discovery tasks require the following permissions:
    - Remote Enable permission on WMI's CIMV2 Namespace
    - Enable Account permission on WMI's CIMV2 Namespace
    - Remote Activation permission on computer via DCOM.

    To set Remote Enable and Enable Account permissions

    1. Open `wmimgmt.msc`.
    2. Right-click **WMI Control (Local)** and select **Properties**.
    3. Select the **Security** tab.
    4. Expand the **Root** node.
    5. Select the **CIMV2** node.
    6. Click the **Security** button.
    7. Add user/group and select **Remote Enable** and **Enable Account**.
    8. Click **OK**.

    To set Remote Activation permissions

    1. Open `dcomcnfg`.
    2. Expand **Component Services** > **Computers**.
    3. Right-click **My Computer** and select **Properties**.
    4. Open the **COM Security** tab.
    5. Under **Launch and Activation Permissions**, select **Edit Limits**.
    6. Add user/group and select **Allow** for **Remote Activation**.
    7. Click **OK**.
- Password change task requires the following permission:
    - Member of Local Administrators group

Domain password management

Using a Domain account:

- Test connection, Check connection, Password check, and Account discovery tasks require the following permissions:
    - Member of Domain Users
- Password change task requires that the Service account has the following delegated permissions:
    - LockoutTime (Read/Write)
    - Account Restrictions (Read/Write)
    - Reset Password

Asset session access

Using a local account:

- Member of Remote Desktop Users group
- Defined in the "Allow log on through Remote Desktop Services" policy (directly or via group membership)
- Not defined in the "Deny log on through Remote Desktop Services" policy (directly or via group membership)

Using a Domain account:

- Defined in the Remote Desktop Users group or be a member of a domain security group by a group policy update to the Remote Desktop Users group for that asset
- Defined in the "Allow log on through Remote Desktop Services" policy (directly or via group membership)
- Not defined in the "Deny log on through Remote Desktop Services" policy (directly or via group membership)

18

Troubleshooting

One Identity recommends the following resolutions to some of the common problems you may encounter as you deploy and use SPP. For more information about how to troubleshoot SPP, refer to the Appliance.

Appliance is sick

Connectivity failures

Cannot connect to remote machine through SSH or RDP

Cannot delete account

Cannot play session message

Domain user denied access to SPP

LCD status messages

My Mac keychain password or SSH key was lost

Password fails for Unix host

Password or SSH key is pending a reset

Password or SSH key profile did not run

Recovery Kiosk (Serial Kiosk)

Replica not adding

System services did not update or restart after password or SSH key change

Test Connection failures

Timeout errors causing operations to fail

User locked out

User not notified

Related Topics

Frequently asked questions

Appliance is sick

There are so many possible root causes for a sick appliance. If you receive an error that the appliance is sick take the following steps.

1. Check network connectivity between nodes.
2. Wait (up to 30m) to see if the error resolves automatically.
3. If the error persists, create a support bundle and contact support. For more information, see Support bundle on page 148.

Categories of appliance sick events by error message prefix

There are 6 categories for appliance sick events which can be distinguished by the error message prefix.

`Audit Log is sick : <reason>`

There is an error in the underlying audit log database. The reason will provide more details about the exact issue. Typically this is due to loss of consensus as a result of network connectivity. This may be the result of temporary network conditions and, if so, it will resolve automatically after a few minutes. If not, check network connectivity between Safeguard nodes. After ruling out network connectivity, generate a support bundle and contact Support. Do not reboot the appliance until consulting with Support. In some cases, rebooting the appliance can make the condition worse.

`Access Request Workflow is sick : <reason>`

There is an error in the underlying password workflow database. The reason will provide more details about the exact issue. Typically this is due to loss of consensus as a result of network connectivity. This may be the result of temporary network conditions and, if so, it will resolve automatically after a few minutes. If not, check network connectivity between Safeguard nodes. After ruling out network connectivity, generate a support bundle and contact Support.

`Policy Data is sick : <reason>`

There is an error in the underlying policy database. The reason will provide more details about the exact issue. Typically this occurs when a replica has lost network connectivity to the primary. This may be the result of temporary network conditions and, if so, it will resolve automatically after a few minutes. If not, check network connectivity between Safeguard nodes. After ruling out network connectivity, generate a support bundle and contact Support.

`Cluster Connectivity is sick : <reason>`

There is an error in the VPN connection between Safeguard nodes. The reason will provide more details about the exact issue. This may be the result of temporary network conditions and, if so, it will resolve automatically after a few minutes. If not, check network connectivity between Safeguard nodes on the public IP address since the VPN is tunneled over the public IP. After ruling out network connectivity, generate a support bundle and contact Support.

Appliance Resource Usage is sick : <reason>

A Safeguard process or underlying database is exhibiting unexpectedly high OS resource usage (CPU, Memory, Disk). The reason will provide more details about the exact issue. Restarting the appliance may resolve this issue. If the problem persists or recurs frequently, generate a support bundle and contact Support.

Connectivity failures

The most common causes of failure in SPP are either connectivity issues between the appliance and the managed system, or problems with service accounts.

Always verify network connectivity and asset power before troubleshooting.

The following topics explain some possible reasons that **Check Password**, **Change Password**, and **Set Password** may fail, and gives you some corrective steps you can take.

- Change password or SSH key fails: Learn about a possible resolution if Change Password fails.
- Incorrect authentication credentials: Learn how to resolve incorrect service account credentials.
- Missing or incorrect SSH host key: Learn how to resolve issues with SSH host keys.
- No cipher supported error: Learn how to resolve cipher support issues.
- Service account has insufficient privileges: Learn how to resolve service account privilege issues.

Change password or SSH key fails

A local account password or SSH key change can fail when you are using a Windows asset that is configured with a service account with Administrative privileges, other than the built-in Administrator.

NOTE: Before SPP can change local account passwords on Windows systems, using a member of an administrators group other than built-in Administrator, you must change the local security policy to disable User Account Control (UAC) Admin Approval Mode (**Run all administrators in Admin Approval Mode**) option.

To configure Windows assets to change account passwords

1. Run `secpol.msc` from the **Run** dialog,

   -OR-

   From the Windows **Start** menu, open **Local Security Policy**.
2. Navigate to **Local Policies** > **Security Options**.
3. Disable the **User Account Control: Run all administrators in Admin Approval Mode** option.
4. Restart your computer.

For more information, see Preparing Windows systems on page 629.

Incorrect authentication credentials

You must have the correct user name and password or SSH key to authenticate to an asset.

To resolve incorrect service account credentials

1. Verify the service account credentials match the credentials in SPP asset information (**Asset Management** > **Assets** > **General Tab, Connection**). For more information, see About service accounts on page 321.
2. Perform **Test Connection** to verify connection. For more information, see About Test Connection on page 322.
3. Attempt to check, change, and set password or SSH keys again. See:
   - Checking, changing, or setting an account password
   - Checking, changing, or setting an SSH key

Missing or incorrect SSH host key

If a SPP asset requires an SSH host key and does not have one, SPP will not be able to communicate with the asset. For more information, see Certificate issue on page 654.

To resolve missing SSH host keys

To verify that an asset has an SSH host key, select the asset and look under **Connection** on the **General** view. If there is no **SSH Host Key Fingerprint** displayed, you need to add one.

To add an SSH host key

1. Open the asset's **Connection** tab.
2. Choose any authentication type (except **None**) and enter required information.

   NOTE: You must enter the service account password or SSH key again.
3. Click **Test Connection**.

   Test Connection verifies that the appliance can communicate with the asset.
4. Confirm that you accept the SSH host key.

   NOTE: To bypass the SSH host key verification and automatically accept the key, click the **Auto Accept SSH Host Key** option.
5. Click **OK** to save asset.

To resolve incorrect SSH host keys

SPPuses the following host key algorithms for key exchange:

- DSA
- ECDSA
- RSA

Investigate the cause of the mismatch and then use **Test Connection** to resolve the mismatch.

No cipher supported error

If you receive an error message that says: `There is no cipher supported by both: client and server`, refer to Cipher support on page 654.

Service account has insufficient privileges

If you are having service account issues, consider the following:

- Is the service account properly authorized to access the system? In a common setup, `sudo` is used to elevate the service account's privileges on the system.
- Has the service account been locked out or disabled?
- Is the service account configured to allow remote logon?

A service account needs sufficient permissions to edit the passwords of other accounts. For more information, see About service accounts on page 321.

To resolve incorrect or insufficient service account privileges

1. Verify that the service account has sufficient permissions on the asset.
2. Perform **Test Connection** to verify connection.
3. Attempt to manually check, change, and set password or SSH key again on the account that failed.

If the asset is running a Windows operating system, a local account password or SSH key check, change, or set can fail when you are using an asset that is configured with a service account with Administrative privileges, other than the built-in Administrator.

Before SPP can change local account passwords or SSH keys on Windows systems, using a service account that is a non-built-in administrator, you must change the local security policy to disable the **Run all administrators in Admin Approval Mode** option. For more information, see Change password or SSH key fails on page 638.

Cannot connect to remote machine through SSH or RDP

If you are unable to connect to a remote machine either through SSH or RDP, log in to the SPP client as an Appliance Administrator and check the Activity Center and logs for additional information.

Cannot delete account

If you are unable to delete an account, review the considerations below.

Wrong account name:

As an Asset Administrator, you may receive this error if you attempt to delete an account : `This entity has access requests which have not yet expired or have to be reviewed. It cannot be deleted now`. This error could indicate that SPP is trying to change the password or SSH key on an account that does not exist on the asset.

One reason for this error message is that the wrong account name was used when adding the account to Safeguard. So now when someone requests the password or SSH key for this account, Safeguard displays the password or SSH key that was manually set. However, when the requester attempts to log in to the asset using the bad account and password or SSH key, it will fail. If the access request policy specified **Change password after check-in**, the above error message appears when the administrator tries to delete the account from SPP.

Workaround: To delete the account with the misspelled name, first manually set the password or SSH key on the account. Once the account password is reset, SPP will allow you to delete the account.

For more information, see:

- Checking, changing, or setting an account password
- Checking, changing, or setting an SSH key

Cannot play session message

If you receive a message that says `Cannot play session... The specified executable is not a valid application for this OS platform`, you are most likely attempting to run the Desktop Player on a 32-bit platform, which is not supported.

Domain user denied access to SPP

If you add a directory user who has the `User must change password at next logon` option enabled in Active Directory, SPP prevents that user from logging in. There are two ways to allow the directory user to log in to SPP successfully:

- Have the directory user use their domain account to log in to an asset joined to Active Directory. When prompted they can change their password. This fulfills the `User must change password at next logon` requirement.

  -OR-

- Have the domain administrator disable the option in Active Directory for the directory user.

LCD status messages

The One Identity Safeguard for Privileged Passwords Appliance has an LCD screen that displays the status of the appliance as it is starting and as it progress through certain operations.

As it proceeds through its various stages, it displays the following LCD status messages. First boot setup refers to the initial configuration of SPP, which normally happens at the factory when the appliance is deployed and after a factory reset.

- **Apply Update xx%**: Shows the percentage completed as the appliance progresses through an update operation.
- **Factory Reset xx%**: Shows the percentage completed as the appliance progresses through a factory reset.
- **First boot ... <version>**: Displays after the first boot completes while it is waiting for SPP to load.
- **First Boot Setup xx%**: Shows the percentage completed as the appliance is being configured for the first time.
- **Preparing for first boot setup**: Displays after a factory reset and before the appliance starts configured for the first time.
- **Quarantine**: Indicates the appliance in a Quarantine state. For more information, see What do I do when an appliance goes into quarantine on page 672.
- **Starting core**: Indicates that SPP is being loaded.
- **Starting database**: Indicates that the SPP database is being loaded.
- **Starting reboot**: Indicates the appliance is being rebooted.
- **Starting services**: Indicates that SPP services are being loaded.
- **Starting shut down**: Indicates the appliance is being shut down.
- **Starting web**: Indicates that the web services are being loaded.

When the appliance is running, the LCD home screen displays: `Safeguard for Privileged Passwords <version number>`.

Appliance LCD and controls

The front panel of the One Identity Safeguard for Privileged Passwords 4000 Appliance, 3000 Appliance and 2000 Appliance contain the following controls for powering on, powering off, and scrolling through the LCD display.

- ✔ Green check mark button: Use the **Green check mark** button to start the appliance. Press the **Green check mark** button for NO more than one second to power on the appliance.

  ⚠ **CAUTION: Once the SPP Appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.**

- Red X button: Use the **Red X** button to shut down the appliance. Press and hold the **Red X** button for four seconds until the LCD displays POWER OFF.

  ⚠ **CAUTION: Once the SPP Appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.**

- Down, up, left, and right arrow buttons: When the appliance is running, the LCD home screen displays: `Safeguard for Privileged Passwords <version number>`. Use the arrow buttons to scroll through the following details:
  - Serial: <appliance serial number>
  - X0: <appliance IP address>
  - MGMT: <management IP address>
  - MGMT MAC: <media access control address>
  - IPMI: <IP address for IPMI>

Table 235: Appliance LCD and controls

Control	Description
Green check mark button	Use the **Green check mark** button to start the appliance. Press the **Green check mark** button for NO MORE THAN one second to power on the appliance. ⚠ **CAUTION: Once the SPP Appliance is booted, DO NOT press and hold the Green check mark button. Holding this button for four or more seconds will cold reset the power of the appliance and may result in damage.**

Control	Description
Red X button	Use the **Red X** button to shut down the appliance. Press and hold the **Red X** button for four seconds until the LCD displays POWER OFF. **CAUTION: Once the SPP Appliance is booted, DO NOT press and hold the Red X button for more than 13 seconds. This will hard power off the appliance and may result in damage.**
Down, up, left, and right arrow buttons	When the appliance is running, the LCD home screen displays: • SPP <version number> Use the arrow buttons to scroll through the following details: • Serial: <appliance serial number> • X0: <appliance IP address> • MGMT: <management IP address> • MGMT MAC: <media access control address> • IPMI: <IP address for IPMI>

My Mac keychain password or SSH key was lost

The keychain in Macintosh OS X is the Apple password and SSH key management system. A keychain can store all your passwords and SSH keys for applications, servers, and web sites, or even sensitive information unrelated to your computer, such as credit card numbers or personal identification numbers (PINs) for bank accounts.

If you have added a Mac OS X system to SPP, you may receive a message that says, `The system was unable to unlock your login keychain`. That is because SPP automatically updates the account passwords on all managed systems based on the policies your Security Policy Administrator has configured, but it does not update the keychain password.

Password fails for Unix host

Some Unix systems silently truncate passwords to their maximum allowed length. For example, Macintosh OS X only allows a password of 128 characters. If an Asset Administrator creates a profile with an Account Password Rule that sets the password length to 136 characters, when SPP changes the password for an account governed by that profile, the asset's operating system truncates the new password to the allowable length

and does not return an error; however, the full 136-character password is stored in SPP. This causes the following issues:

- Check Password for that account will fail. When SPP compares the password on the Unix host with the password in SPP, they never match because the Unix host truncated the password generated by SPP.
- A user will not be able to log in to the Unix host account successfully with the password provided by SPP unless they truncate the password to the allowable length imposed by the operating system.

Password or SSH key is pending a reset

If a user receives a persistent message that states either of the following types of messages, the account password or SSH key is stuck in a pending password/SSH key change state:

- `You cannot checkout the password or SSH key for this account while another request is pending password or SSH key reset`
- `This account has password or SSH key requests which have not yet expired or have to be reviewed. It cannot be deleted now"`

Possible solutions:

- Ensure that the service account for the asset associated with this account is working. Then manually change the account password or SSH key . See: Checking, changing, or setting an account password and Checking, changing, or setting an SSH key.
- Or, if the service account for the asset is working properly and the policy governing the account allows emergency access and has enabled multiple users simultaneous access, you can instruct the user to request the password or SSH key using Emergency Access.

You can allow new access requests whether a prior request is approved or not approved. In other words, no requests will be blocked based on the approval status of a prior request. Setting the **Pending reviews do not block access** check box only pertains to future requests. For more information, see Workflow tab (create access request policy).

Password or SSH key profile did not run

The password and SSH key management settings enable the automatic profile check and change schedules in partitions. For more information, see Global Services.

Ensure the password and SSH key management settings are enable for profiles to run on schedule:

- Check Password Management Enabled
- Change Password Management Enabled
- Check SSH Key Management Enabled
- Change SSH Key Management Enabled

Recovery Kiosk (Serial Kiosk)

SPP provides a Recovery Kiosk (Serial Kiosk) with the following options.

- Appliance information (Recovery Kiosk): Allows you to view basic appliance information.
- Backups: Allows you to access backups from quarantined appliances.
- Power options: These options allow you to remotely restart or shut down the appliance.
- Admin password reset: Allows you to reset the Bootstrap Administrator's password to its initial value.
- Factory reset from the Recovery Kiosk: Allows you to recover from major problems or to clear the data and configuration settings on the appliance.

  Factory reset is not available for virtual appliances. Virtual appliances are backed up and can be recovered. For more information, see Virtual appliance backup and recovery on page 68.

  > **CAUTION: Care should be taken when performing a factory reset against a physical appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. Performing a factory reset will NOT reset the BMC/IPMI interface or the IP address. However, the BMC/IPMI interface will need to be reenabled after the reset has completed (for more information, see Lights Out Management (BMC)). The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.**
  >
  > **In addition, performing a factory reset may change the default SSL certificate and default SSH host key.**
  >
  > **The appliance resets to the current Long Term Support (LTS) version. For example, if the appliance is running version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, the appliance will reset down to 6.0 LTS and you will have to patch up to your desired version. For more information, see Long Term Support (LTS) and Feature Releases on page 42.**

- Support bundle: Allows you to generate and send a support bundle to a Windows share.

To start the Recovery Kiosk

On the terminal or laptop running the Recovery Kiosk, you must configure your serial port settings as follows:

1. Connect a serial cable from a laptop or terminal to the serial port on the back of the appliance marked with **|0|0|**.
2. On the laptop or terminal, configure the serial port settings as follows:
    - Speed: 115200
    - Data bits: 8
    - Parity: None
    - Stop bit: 1
3. These options display on the Recovery Kiosk screen:
    - **Appliance Information**
    - **Backups**
    - **Power Options**
        - **Reboot**
        - **Shut Down**
    - **Admin Password Reset**
    - **Factory Reset** (Not available for virtual appliances.)
    - **Support Bundle**
4. Use the up-arrow and down-arrow to select one of these options.
5. Use the right-arrow to initiate the option.
6. Use the left-arrow to return to the option.

Kiosk keyboard shortcuts

SPP provides these keyboard shortcuts. If you make the window too small to accommodate the kiosk elements, SPP tells you how to readjust the window size.

- **Ctrl+D**: Resets the kiosk to its original state.
- **Ctrl+R**: Redraws the kiosk to fit a resized window. If you resize the window, press **Ctrl + R** to reorganize the kiosk elements to fit properly into the newly-sized window.

Appliance information (Recovery Kiosk)

Use the **Appliance Information** option on the Recovery Kiosk to view basic appliance information and edit the IP addresses.

If you are using Azure, configure the SPP VM with a static IP address in Azure. If you need to change the IP address of the Safeguard appliance, or if it changes due to dynamic

configuration in Azure, and the appliance is part of a cluster, the appliance will automatically reset to Standalone Read-only mode on the next boot (effectively leaving the cluster). The Administrator can join the appliance back to the cluster.

To view or edit the appliance information

1. From the Recovery Kiosk, select the **Appliance Information** option.
2. Right-arrow to see:
    - Appliance State: The appliance's current state.
    - Uptime: The amount of time (hours and minutes) the appliance has been running.
    - MGMT (not used Azure): The management host's network interface properties, including the MAC address and IPv4 (and optionally IPv6) properties.
    - X0: The network interface properties for the primary interface that connects your appliance to the network, including the MAC address and IPv4 (and optionally IPv6) properties.
3. To change the network properties for the primary interface (XO), click **Edit** next to the appropriate heading. Clicking **Edit** displays the network interface properties which can be modified. If you are using Azure, the IP address cannot be changed.
4. After editing the network interface properties, click **Submit**.

   Once the updates are completed, a `Network interface update request accepted` message is displayed.

Backups

This page allows you to access backups from quarantined appliances, so long as the appliance is not rebooted.

Accessing backup from quarantined appliance

1. Connect to the recovery Kiosk, either physically via serial cable or via the IPMI network interface.
2. From the Recovery Kiosk, select the **Backups** option.
3. Press the **Enter** key (or right arrow).
4. At **Name or Email**, enter your identification and press the **Tab** key (or down arrow).
5. Select **Submit**.
6. At **View Challenge**, press the **Enter** key.

   SPP produces a challenge.
7. Copy and paste the challenge into a text document and send it to One Identity Support.
    - A challenge response is only good for 48 hours.

8. When you get the response from One Identity Support, select **Enter Response** and copy and paste the response into the kiosk screen.
9. Select **Authorize Backups**. The response is only valid for 24 hours from when it was generated by One Identity.
10. The **Backups** page will display any previously generated backups. You will only have 24 hours after the successful authorization to access the backups. The following options are available:
    - Select a backup to copy to a CIFS share:
        a. Select the backup and press the **Enter** key.
        b. Enter the UNC path and login credentials.
        c. Select **Submit**.
        d. Once the backup has been copied, select **Close**.
    - **Delete Authorization**: Select this option to delete the authorization granted by the challenge response process. Once deleted, you will be unable to access the backups page until a new challenge response has been successfully completed.

Power options

Use the power options in the Recovery Kiosk to remotely restart or shut down the physical appliance or AWS or Azure virtual deployment.

- You can use the **Reboot** option in the Recovery Kiosk to restart the appliance. Reboot from the Recovery Kiosk if you cannot access the SPP web client or API to restart the appliance using the normal procedures. Reboot the AWS or Azure virtual deployment.
- You must use the **Shut Down** option in the Recovery Kiosk to shutdown the physical appliance or AWS or Azure virtual deployment.

Rebooting the appliance

Restarting the appliance from the Recovery Kiosk is available.

If you cannot access the SPP web client or API to restart the appliance using the normal procedures, you can restart the appliance or Azure VM from the Recovery Kiosk.

To reboot the appliance

1. From the Recovery Kiosk, select the **Power Options** > **Reboot** option.
2. Press the right arrow.
3. When prompted, select **Yes** to start the reboot or **No** to return to the main option screen.

Shutting down the appliance

Shutting down the appliance from the Recovery Kiosk is available. You must use the Recovery Kiosk to manually shutdown the One Identity Safeguard for Privileged Passwords Appliance. You can also shut down the Azure virtual machine deployment.

To shut down the appliance

1. From the Recovery Kiosk, select the **Power Options** > **Shut Down** option.
2. Press the right arrow.
3. When prompted, select **Yes** to shut down the appliance or **No** to return to the main option screen.

Admin password reset

If your Bootstrap Administrator's password is locked out when using the hardware appliance or AWS or Azure virtual deployment, you can reset it to the initial password.

NOTE: If a user has not logged onto SPP for a set number of days, SPP disables the user account. This is set using the **Deactivate After** setting in **Appliance Management** > **Safeguard Access** > **Local Login Control**.

To reset the Bootstrap Administrator's password

1. Connect to the recovery Kiosk, either physically via serial cable or via the IPMI network interface.
2. From the Recovery Kiosk, select the **Admin Password Reset** option.
3. Press the **Enter** key (or right arrow).
4. At **Name or Email**, enter your identification and press the **Tab** key (or down arrow).
5. Select **Submit**.
6. At **View Challenge**, press the **Enter** key.

   SPP produces a challenge.
7. Copy and paste the challenge into a text document and send it to One Identity Support.
   - A challenge response is only good for 48 hours.
8. When you get the response from One Identity Support, select **Enter Response** and copy and paste the response into the kiosk screen.
9. Select **Reset Password**. The response is only valid for 24 hours from when it was generated by One Identity.
10. Once the operation has completed, the password for the admin account is defaulted back to **Admin123**

NOTE: **Best practice**: To keep your appliance secure, change the default password for the Bootstrap Administrator's account.

See the following Knowledge Base Article for more information, including using the MGMT port to reset the admin password: KB 279291: How to reset the Admin password.

Factory reset from the Recovery Kiosk

There is a **Factory Reset** selection in the Recovery Kiosk. **Factory Reset** allows you to reset a SPP hardware appliance to recover from major problems or to clear the data and configuration settings on the appliance.

Factory reset is not an option for virtual appliances. You will need to redeploy the appliance.

CAUTION: Care should be taken when performing a factory reset against a physical appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. Performing a factory reset will NOT reset the BMC/IPMI interface or the IP address. However, the BMC/IPMI interface will need to be reenabled after the reset has completed (for more information, see Lights Out Management (BMC)). The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

The appliance resets to the current Long Term Support (LTS) version. For example, if the appliance is running version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, the appliance will reset down to 6.0 LTS and you will have to patch up to your desired version. For more information, see Long Term Support (LTS) and Feature Releases on page 42.

Factory reset on a clustered appliance

Performing a factory reset on a clustered hardware appliance will not automatically remove the appliance from a cluster. The recommended best practice is to unjoin an appliance from the cluster before performing a factory reset on the appliance. After the unjoin and factory reset, the appliance must be configured again. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.

To perform a factory reset from the Recovery Kiosk

CAUTION: As part of the factory reset process, you will be performing a challenge response operation.

If the challenge response operation is invalidated, try restarting the process to generate a new challenge response. If that fails, contact One Identity Support for assistance.

1. To perform a hardware factory reset, go to the Recovery Kiosk. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.
2. Select **Factory Reset**.
3. Press the right arrow.
4. At **Name or Email**, enter your email or name and press the **Tab** key (or down arrow).
5. Select **Submit**.
6. At **View Challenge**, press the **Enter** key. Safeguard for Privileged Passwords produces a challenge. (If the challenge is not shown, maximize Putty.)
7. Copy and paste the challenge into a text document and send it to One Identity Support. A challenge response is only good for 48 hours.

   IMPORTANT: Do not reboot the machine during the challenge response process.
8. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select **Factory Reset**. The response is only valid for 24 hours from when it was generated by One Identity.
9. Once the factory reset is completed the appliance will need to be reconfigured.

See the following Knowledge Base Article for details on using the MGMT network interface for factory reset: KB 232766: What are the steps to perform a factory reset from the recovery kiosk or MGMT network interface on physical devices?

Support bundle

Prior to using the **Support Bundle** function, set up a Windows share where the support bundle is to be sent.

To generate a support bundle

1. From the Recovery Kiosk, select the **Support Bundle** option.
2. Press the right arrow.
3. Select the type of support bundle to be generated:
   - Support Bundle
   - Quarantine Bundle
4. When prompted, enter the following information:
   - Address: Enter the address of the Windows share (`<IP Address>\<ShareName>`) where the support bundle is to be saved.
   - User: Enter the user name to be used to access the Windows share.
   - Password: Enter the password associated with the specified user account.

     NOTE: If you set up the Windows share to allow anonymous access, you will not be prompted to enter a user name or password.

5. Select **Copy to Share**. When completed, a message appears stating that a support bundle has been sent to the specified share.

Replica not adding

If you receive a persistent message that says, `An internal request has timed out...` when you attempt to add an appliance to a cluster, ensure that the appliance is at the same version of SPP as the primary. All members of a cluster must be the same.

System services did not update or restart after password or SSH key change

If the system services do not update or restart after an automatic password or SSH key change, first check your audit logs in the Activity Center.

NOTE: You can also check the Support bundle logs.

If the audit logs do not adequately explain the problem, then check the options on the **Change password** or **Change SSH key** tab of the profile that governs the service account.

1. Navigate to **Asset Management** > **Partitions**.
2. Select a partition then click **Password Profiles** or **SSH Key Profiles**.
3. Double-click the selection in the grid.
4. On the profile dialog, go to the **Change Password** or **Change SSH Key** tab.

For service accounts that run system services or scheduled system tasks, verify the options on the profile's **Change password** tab or **Change SSH Key** tab that enable or disable automatic service update, or restart. You must update the setting to change these options.

Test Connection failures

The most common causes of failure in SPP are either connectivity issues between the appliance and the managed system, or problems with service accounts.For more information, see Connectivity failures on page 638.

Disabling User Account Control (UAC) Admin Approval Mode on a remote host can also resolve **Test Connection** failures. For more information, see Change password or SSH key fails on page 638.

If you have entered values for **Specify Domain Controllers** and if SPP does not find a domain controller in the list, the test connection fails and an error is returned.

The following topics explain some possible reasons that **Test Connection** could fail.

- Test Connection failures on archive server: Learn how to resolve **Test Connection** failures for archive servers.
- Certificate issue: Learn how to resolve **Test Connection** failures for assets that require SSL.
- Cipher support: Learn about SPP's cipher support.
- Domain controller issue: Learn how SPP manages passwords for accounts on domain controllers.
- Networking issue: Learn how to resolve system connectivity issues.
- Windows WMI connection: Learn how to enable SPP to manage Windows assets.

Test Connection failures on archive server

There could multiple reasons why you receive an `Unexpected copying error...` when attempting to run **Test Connection** on an existing archive server.

When you run **Test Connection**, SPP adds a file named `Safeguard_Test_Connection.txt` to the **Storage Path** location of the archive server owned by the **Account Name** you entered when you created the archive server. To run **Test Connection** on an existing archive server with a new account name, you must first delete the existing `Safeguard_Test_Connection.txt` file.

Certificate issue

If you are experiencing **Test Connection** failures for an asset that uses SSL, these are some possible causes:

- The asset's signing authority certificate has not been added to the Trusted CA Certificates store in SPP.
- The signing authority's certificate has expired.
- There is a name mismatch between the name given and the name on the certificate of the asset. For more information, see Missing or incorrect SSH host key on page 639.

Cipher support

Both the SPP client and the SSH server must support the same cipher. If you run **Test Connection** against an asset that uses SSH and there is no cipher supported by both the

client and the server, SPP displays an error message that says, `Connecting to asset XXXXXXXXXXXXXXXXXX failed (There is no cipher supported by both: client and server)`. This means that during the setup of the asset connection, the SPP client and the SSH server did not have matching ciphers for message encryption. In this case, you must modify the SSH server's configuration by adding at least one cipher supported by SPP to the list of ciphers.

SPP supports these ciphers:

- 3des
- 3des-ctr
- aes128
- aes128-ctr
- aes192
- aes192-ctr
- aes256
- aes256-ctr
- arcfour
- arcfour128
- arcfour256
- blowfish
- blowfish-ctr
- cast128
- cast128-ctr
- des
- idea
- idea-ctr
- none
- serpent128
- serpent128-ctr
- serpent192
- serpent192-ctr
- serpent256
- serpent256-ctr
- twofish128
- twofish128-ctr
- twofish192
- twofish192-ctr

- twofish256
- twofish256-ctr

For example, if using an OpenSSH server with a default list of ciphers, you must add one or more of these ciphers in the OpenSSH's `sshd_config` file, and then restart the SSH server. For more information about OpenSSH ciphers, see http://www.openbsd.org/cgi-bin/man.cgi/OpenBSD-current/man5/sshd_config.5?query=sshd_config&sec=5.

Domain controller issue

SPPdoes not manage passwords for accounts on domain controllers; SPP manages passwords for accounts on a domain controller through a directory that hosts the domain controller. For more information, see Adding an account on page 286.

Networking issue

If you are having system connectivity issues, here are some things to consider:

- Are there security rules on the network (such as firewalls or routers) that might be preventing this traffic?
- Is traffic from SPP routable to the network address of the managed system?
- Are there any problems with cables, hubs, or switches, and so forth?

You could be experiencing network issues like these:

- Network outage
- Router misconfiguration
- Unplugged wire
- Switch not working

If Safeguard for Privileged Passwords suspends event notifications, try logging out and logging back in to re-subscribe to SignalR.

Windows WMI connection

To enable SPP to manage Windows assets, you must configure your firewall to allow Windows Management Instrumentation (WMI).

Timeout errors causing operations to fail

If you experience any timeout errors, wait a few minutes and retry the operation.

If you are performing clustering operations in the background, for example adding replicas to a cluster, wait for the cluser operations to complete before performing other operations in SPP.

> TIP: A timeout error can appear as a `Request failed. A task was canceled.` error message.

User locked out

If a user has not logged on to SPP for a set number of days, SPP disables the user account.

> NOTE: This is set using the **Deactivate After** setting in **Appliance Management** > **Safeguard Access** > **Local Login Control**. For more information, see Local Login Control on page 247.

Related Topics

Unlocking a local user's account

User not notified

If a user did not receive an email notification, first check to see if you have set everything up in SPP correctly for the email notifications to work properly. For more information, see Enabling email notifications on page 219.

Notification lists

SPP does not dynamically maintain the email addresses for an escalation notification contact list.

If you change a SPP user's email address or delete a SPP user after creating a policy, you must update the email addresses in escalation notification contact lists manually. For example, when you create a policy, you can indicate who to contact when emergency access has been used. If a user has changed an email address, the notification will not be received by that individual. Furthermore, if a user has been deleted from SPP, the user will still receive the notification.

Frequently asked questions

The following topics will help you find answers to some of your questions about managing SPP:

How do I audit transaction activity
How do I configure external federation authentication
How do I manage accounts on unsupported platforms
How do I modify the appliance configuration settings
How do I prevent SPP messages when making RDP connections
How do I set up telnet and TN3270/TN5250 session access requests
How do SPP database servers use SSL
What are the access request states
What do I do when an appliance goes into quarantine
When does the rules engine run for dynamic grouping and tagging
Why did the password or SSH key change during an open request

Related Topics

Appliance
Troubleshooting

How do I audit transaction activity

The appliance records all activities performed within One Identity Safeguard for Privileged Passwords. Any administrator has access to the audit log information; however, your administrator permission set determines what audit data you can access.For more information, see Administrator permissions on page 604.

SPPprovides several ways to audit transaction activity:

- Password Archive: Where you access a previous password for an account for a specific date. For more information, see Viewing password archive on page 292.
- SSH Key Archive: Where you access a previous SSH key for an account for a specific date. For more information, see Viewing SSH key archive on page 294.
- Check and Change Log: Where you view an account's password and SSH key validation and reset history. Access the **Check and Change Log** from **Accounts**. For more information, see Accounts on page 273.
- History: Where you view the details of each operation that has affected the selected item. For more information, see History tab (account) on page 285.
- Activity Center: Where you can search for and review any activity for a specific time frame. For more information, see Activity Center on page 564.
- Work flow: Where you can audit the transactions performed as part of the workflow process from request to approval to review for a specific access request. For more information, see Auditing request workflow on page 570.
- Reports: Where you can view and export entitlement reports that show you which assets and accounts a selected user is authorized to access. For more information, see Reports on page 563.

How do I configure external federation authentication

One Identity Safeguard for Privileged Passwords supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different Identity Provider STS servers and services, such as Microsoft's AD FS. Through the exchange of the federation metadata, you can create a trust relationship between the two systems. Then, you will create a SPP user to be associated with the federated user.

Safeguard supports both Service Provider (SP) initiated and Identity Provider (IdP) initiated logins.

- For SP initiated, the user will first browse to Safeguard and choose **External Federation** as the authentication provider. After entering just their email address, they will be redirected to the external STS to enter their credentials and perform any two-factor authentication that may be required by that STS. After successful authentication, they will be redirected back to Safeguard for Privileged Passwords and logged in.
- For IdP initiated logins, a user will first go to their IdP STS and authenticate. Typically, the customer will have configured Safeguard as an application within their STS, allowing the user to just click on a link or icon and be redirected to Safeguard, automatically being logged in without having to enter any further credentials.

NOTE: Additional two-factor authentication can be assigned to the associated SPP user to have the user authenticate again after being redirected back from the external STS.

To use external federation, you must first download a copy of, or have the URL to the federation metadata XML of your STS. For example, in Microsoft AD FS, you can download the federation metadata XML from: `https://<adfs server>/FederationMetadata/200706/FederationMetadata.xml`. Or if the SPP appliance can directly access that URL, it can be used as well when creating the provider.

How do I add an external federation provider trust

It is the responsibility of the Appliance Administrator to configure the external federation service providers in SPP.

To add an external federation service provider

1. Go to **Appliance Management** > **Safeguard Access** > **Identity and Authentication**.
2. Click + **Add** then select **External Federation**.
3. In the **External Federation** dialog, supply the following information:
   a. **Name**: Enter a unique display name for the external federation service provider. The name is used for administrative purposes only and will not be seen by end users.

      Limit: 100 characters

   b. **Realm**: Enter a unique realm value, typically a DNS suffix, like `contoso.com`, that matches the email addresses of users intended to use this STS for authentication. Values can be separated by a space, comma, or semi-colon. A case-insensitive comparison will be used on the value(s) when performing Home Realm Discovery.

   c. Federation Metadata: Select one of the following options:

      i. **From File**: When using this option, SPP stores a static copy of the metadata. It is the responsibility of the administrators to update the metadata, when necessary, by repeating this process. For example, when the signing certificate used by the STS changes.

         You must first download the federation metadata XML for your STS and save it to a file locally. For example, for Microsoft's AD FS, you can download the federation metadata XML from: `https://<adfs server>/FederationMetadata/2007-06/FederationMetadata.xml`.

         Click **Browse** to select the STS federation metadata xml file.

      ii. **From URL**: When using this option, SPP will automatically download the STS metadata and refresh it on a periodic basis, so it should always have the current signing certificates and other information used by the STS.

         Specify the complete HTTPS URL to the STS metadata. The SSL/TLS certificate used by the HTTPS URL must be trusted on every node of the

SPP cluster, and each node of the cluster will need network/internet access to be able to download from the specified HTTPS URL. It is strongly recommended to verify that you can successfully log in on each node of the cluster after initially creating the Identity Provider.

After the external federation provider is created, you can manually trigger SPP to update the metadata from the configured URL by clicking the **Update Metadata** button. This may be useful to help minimize any downtime when you know that the STS metadata has changed.

> NOTE: A proxy server may be configured. For more information, see Networking.

d. **Download Safeguard Federation Metadata**: If you have not done so before, click the link to download a copy of SPP's federation metadata XML. You will need this file when creating the corresponding trust relationship on your STS server.

> NOTE: The federation metadata XML files typically contain a digital signature and cannot be modified in any way, including white space. If you receive an error regarding a problem with the metadata, ensure that it has not been edited.

e. Click **OK**.

How do I create a relying party trust for the STS

The process for creating the relying party trust in your STS (Security Token Service) will differ between applications and services. However, as stated earlier, you can download a copy of SPP's federation metadata by clicking the link when you entered the STS information in SPP. You can also download the SPP federation metadata at any time using one of the following methods:

1. Go to **Appliance Management** > **Safeguard Access** > **Identity and Authentication**.
2. Click **Download Safeguard Federation Metadata**.
3. Download the file from the following URL:

   https://<SPP server>/RSTS/Saml2FedMetadata

If the STS does not support importing federation metadata, but instead requires you to manually input values, you will typically need an App ID and Login or Redirect URL. Both of these values can be copied from the SPP federation metadata XML file you downloaded.

- The App ID for SPP will come from the `entityID` attribute of the `<EntityDescriptor>` element in the XML file.
- The Login or Redirect URL will come from the `Location` attribute of the `<AssertionConsumerService>` element within the `<SPSSODescriptor>` element.

NOTE: Only the `HTTP-POST` binding is supported for this end point.

NOTE: If using SPP in a clustered environment and you do not use a load balanced DNS name to access SPP, or you wish to be able to log in to a specific node of the cluster, you will have to add additional login redirect URLs to your STS configuration.

You must then configure or ensure that the STS returns the authenticated user's email address as a SAML attribute claim. The email address must appear in either the standard SAML email address claim or name claim:

- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
- http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

If the emailaddress and name attribute claims are not present in the SAML assertion, the SAML Subject NameID can be used.

NOTE: Any other attributes or claims will be ignored.

The SAML Response or Assertion must be signed, but not encrypted. When the signing certificate used by your STS expires, you may need to update the metadata for the associated external federation provider in SPP depending on how it and your STS are configured:

- If the external federation provider in SPP was configured by uploading a copy of the STS metadata file, then that needs to be repeated with the new copy of the STS metadata file containing the new signing certificate.
- If the external federation provider in SPP was configured to use the URL that points to the STS metadata (and the STS supports having multiple active signing certificates for seamless rollover), then you shouldn't have to do anything. SPP periodically attempts to download the metadata and will use the new certificate when it becomes active. Otherwise, you can manually trigger SPP to download and refresh the STS metadata from the configured URL by selecting the external federation provider and clicking the **Update Signing Certificates and Metadata** toolbar button.

NOTE: Your STS's metadata can contain more than one signing certificate to allow for a grace period between an expiring certificate and a new one.

For further details regarding specific STS servers, see the following knowledge base articles on the One Identity support site:

- Configuring Microsoft's AD FS Relying Party Trust for SPP: KB Article 233669
- Configuring Microsoft's Azure AD for SPP: KB Article 233671

How do I add an external federation user

It is the responsibility of either the Authorizer Administrator or the User Administrator to add an associated external federation SPP user.

Preparation

You must add external federation service providers to SPP before you can add external federation users.

No user information, such as first name, last name, phone number, email address, is ever imported from the STS claims token. You must enter that information manually when creating the user in SPP if you need it.

To add a user

1. Navigate to **User Management** > **Users**.
2. In **Users**, click **+New User** from the toolbar.
3. In the User dialog, provide information in each of the tabs:
    - Identity tab (add user): Where you define the identity provider and the user's contact information.
    - Authentication tab (add user): Where you define the authentication provider, login name and password, if necessary.
    - Permissions tab (add user): Where you set the user's administrator permissions.

How do I manage accounts on unsupported platforms

SPP makes it possible for you to manage passwords and SSH keys for accounts on unsupported platforms and not addressed by a Custom platforms.

You will use a profile with a manual change password or an SSH key setting.

For example, you may have an asset that is not on the network. The manual change password or SSH key setting allows you to comply with your company policies to change account passwords on a regular schedule without using the SPP automatic change password or SSH key settings. SPP notifies you by email, toast notification, or both on a set schedule to change account passwords manually. You can then reset the password or SSH key yourself, or allow SPP to generate a random password or SSH key according to the password rule selected in the profile.

> IMPORTANT: After you change the password or SSH key in SPP you must remember to change the password or SSH key on the account; SPP does not do that automatically for you.

The following summarizes the general workflow for managing accounts on unsupported platforms.

To manage account passwords or SSH key manually

1. Configure a profile with a manual change password or SSH key setting and assign asset accounts to it. See: Adding change password settings and Adding SSH key change settings.
2. Ensure toast notifications or email notifications are properly configured. For more information, see Enabling email notifications.
3. When notified to change an account password or SSH key, choose:
   - **Set Password**: **Manual Password** or Generate Password. For more information, see Checking, changing, or setting an account password on page 291.
   - **Set SSH Key**: **Manual SSH Key** or **Generate SSH Key**. For more information, see Checking, changing, or setting an SSH key on page 292..

How do I modify the appliance configuration settings

NOTE: This topic assumes you have already performed the initial appliance installation and configuration steps in the *One Identity Safeguard for Privileged Passwords Appliance Setup Guide* provided in the box with your hardware equipment.

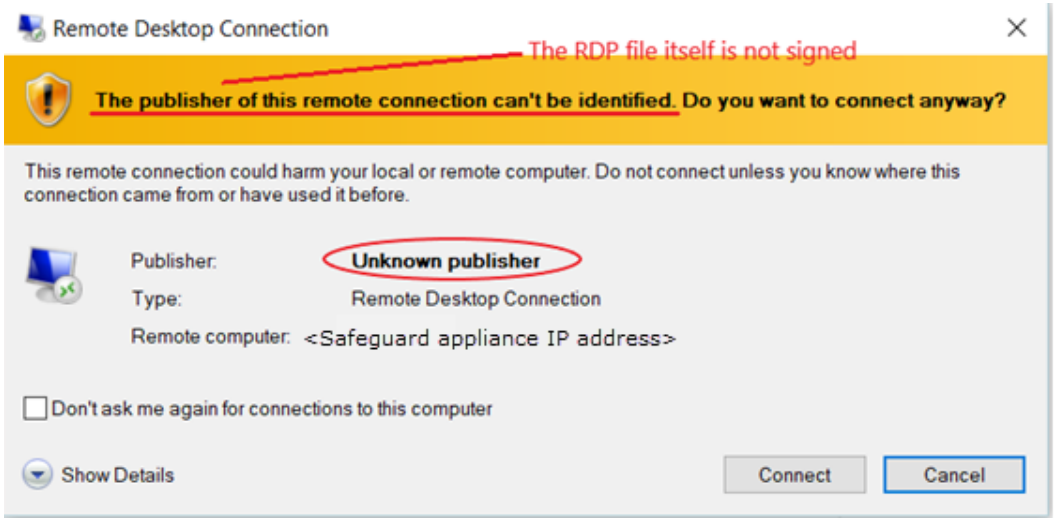
(web client) To modify the appliance configuration settings

1. Log in to the SPP web client using the Appliance Administrator account.
2. Click **Appliance Management** > **Appliance** page.
3. Click **Networking** to configure the appliance. For more information, see Networking on page 141.
   a. On the Appliance Configuration page, configure the following:
      - **Network (X0)**: Enter the DNS Server address information for your primary interface.
   b. Click **Save**.
4. Click **Time** to enable and view information about the Network Time Protocol (NTP):
   a. Select **Enable NTP**.
   b. Set the primary and secondary NTP servers, if desired.
   c. The **Last Sync Time** is displayed. To view or hide details, click **Show Last Sync Details** or **Hide Last Sync Details**. For more information, see Time on page 149.
   d. Click **Save**.

How do I prevent SPP messages when making RDP connections

When making an RDP connection, you may encounter two different certificate messages.

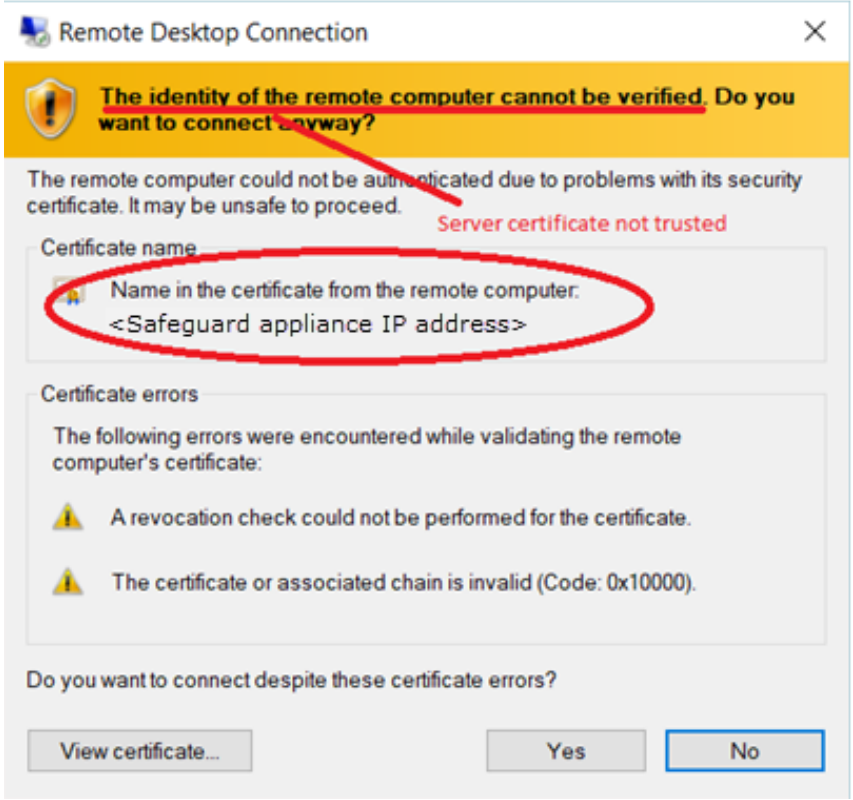
- Unsigned RDP file message



  This message occurs when Remote Desktop Connection opens the RDP file that is downloaded when you click ▶ **Play** in the SPP user interface.

  We are currently working on a solution that will allow SPP to sign this RDP file to avoid this message.

- Untrusted server certification message



This message occurs when the workstation has not trusted the SPP RDP Connection Signing Certificate.

NOTE: The IP address of the connecting server is that of the Safeguard appliance.

To avoid this message, you must trust the RDP Connection Signing Certificate and certificates in its chain of trust or replace the current certificate with an enterprise certificate and chain of trust that is trusted.

One Identity recommends that you replace the entire configuration with your own trusted enterprise PKI. This would result in a structure such as:

- Your Root CA
    - Your Issuing CA
        - Your RDP Signing Certificate (from Safeguard CSR)
            - *<Sessions module generated certificate>*

The Root CA, Issuing CA, and RDP Signing Certificates can be distributed via Group Policy, Active Directory, or other distribution means.

How do I set up telnet and TN3270/TN5250 session access requests

One Identity Safeguard for Privileged Passwords supports session access requests with mainframes using software terminal emulation including telnet and TN3270/TN5250 over telnet. Safeguard for Privileged Sessions version 6.1 or higher is used for session recording.

Actions

- Security officers can record activities of administrators who maintain critical systems running on IBM iSeries and mainframe computers.
- Asset Administrators can:
  - Customize the TN3270/TN5250 login screen field detection to work for the Safeguard custom login setup.
  - Mark an asset as supporting telnet sessions and specify if the asset is available.
- Security Policy Administrators can create an entitlement with an access policy that includes session access using telnet and TN3270/TN5250 sessions over telnet.
- Requesters' log in experience follows the regular client telnet or TN3270/TN5250 interface even when the session is being recorded. Sessions are not launched from SPP and all required log in information is available through SPP.

Steps for sessions access requests using telnet and TN3270/TN5250 over telnet

IMPORTANT: Assistance with One Identity Professional Services is required for help with configurations and installation including available plug-ins, policy creation, pattern files, shortcuts, and best practices.

Safeguard for Privileged Sessions set up steps

Complete the following set up steps in Safeguard for Privileged Sessions (SPS). For operation details, see the *One Identity Safeguard for Privileged Sessions Administration Guide*: One Identity Safeguard for Privileged Sessions Administration Guide.

- Import the necessary plug-in to supply authentication and authorization (AA) and credential store (credstore) information to authenticate with and pull the credentials from SPP. The plug-in file and instructions are available at the Safeguard Custom Platform Home wiki on GitHub.
- Create and assign **Pattern Sets** that use pattern files specific to the log in experience for each connection. A pattern file describes the log in experience for a specific system. The pattern file may include the on-screen location of the user name, password or SSH key field location, login result, descriptions, states, and other required detail. Because log in experiences vary from mainframe to mainframe,

custom pattern files must be created, uploaded, and referenced by the system-related connection policy. Template pattern files and instructions are available at the Safeguard Custom Platform Home wiki on GitHub.

CAUTION: Template pattern files are provided for information only. Customized telnet and TN3270/TN5250 pattern files need to be created. Updates, error checking, and testing are required before using them in production.

- Specify each **Authentication Policy** and list the authentication methods that can be used in a connection.
- Create and configure each **Connection Policy**. Multiple connection policies are typically required because of the uniqueness of each system log on experience and related pattern file as well as the fact that inband destinations are not used for TN3270/TN5250 over telnet.
  For example, telnet can be used for inband destinations. However, inband destinations are not used for TN3270/TN5250 over telnet. Instead, a fixed address including the port and server can be identified which results in the need for a different connection policy for each mainframe. A fixed address in Safeguard for Privileged Sessions includes the port used; the SPP asset port is not used in the connection but is usually the same.
- Export a configuration file, if desired.
- Configure basic settings for the SSH server, cluster interface, and cluster management.

SPP set up steps

Complete the following set up steps in SPP.

- The Asset Administrator adds the mainframe asset including the **Telnet Session Port** that is identified on the **Asset Management** > **Asset** > **Management** tab. For more information, see Adding an asset.
- The Security Policy Administrator sets the **Access Type** (**Telnet**) on the **Security Policy Management** > **Entitlements** > **Access Request Policies** tab.

SPP requester steps

In SPP after all configuration is complete, the requester proceeds based on the terminal service application in use.

- For a terminal service application that uses an inband connection string (like telnet), click **Copy** to copy the **Hostname Connection String** and check out the password or SSH key. Then, paste the information in the log in screen.
- If the terminal service application requires more information for log in (for example, TN3270/TN5250 over telnet):
  - Click **Show** to display values that may include **Vault Address** (the SPP address), a one-time **Token**, **Username**, **Asset**, and **Sessions Module** (the Safeguard for Privileged Sessions address).

- Click **Copy** by any of the values to copy a single value. Or, you can click **Copy** at the right of all values to copy the entire the connection string, if that is required by your terminal service application.
- Paste the necessary information into your terminal service application.

- Click **Check-In Request** to complete the password or SSH key check out process. This makes the session request available to reviewers.
- Click **Hide** to conceal the information from view.

> NOTE: The user would copy an entire connection string if, for example, you have a launcher to take the connection string and launch the profile of the terminal service application.

How do SPP database servers use SSL

Some database servers use Secure Socket Layer (SSL) when communicating with SPP. Depending on the platform type, version, and configuration, the database server can either use SSL for only encrypting the session or it can use SSL for encrypting and verifying the authenticity of the database server.

ODBC Transport

The following platforms use the ODBC transport. SPP installs the appropriate software driver on the appliance to communicate with the platform. The configuration data that SPP uses to initialize a connection with the server is in the form of a connection string consisting of a colon-separated list of driver-specific options.

By default, the database servers encrypt the login data, but not the subsequent data passed on the connection. You must configure SSL and enable it on the database server to enable encryption for the session data.

Microsoft SQL Server

MicrosoftSQL Serveris always capable of encrypting the connection with SSL. It listens on a single port for both SSL and non-SSL connections.

If you have set the Force Encryption option to *yes* on the SQL server, then it uses SSL to encrypt the data, regardless of whether the SPP client requests it or not.

You can set the Force Encryption option to `yes` on the SQL server without configuring a server certificate. In this case, the SQL server transparently generates a self-signed certificate to use when a SPP client requests encryption. This makes it possible for the SQL server to use SSL only to provide encryption for the session without verifying the server certificate.

NOTE: It is not possible from within a running session to detect whether the SQL server is using SSL for encryption.

Table 236: Microsoft SQL Server SSL support

SPP Client Options		Microsoft SQL Server Configuration		Result
Use SSL Encryption	**Verify SSL Cert**	**Force Encryption**	**Server Cert Configured**	
No	n/a	No	n/a	The SQL Server does not encrypt the session.
Yes	No	n/a	No	SPP requests that the SQL server encrypt the session using a generated self-signed certificate.
Yes	No	n/a	Yes	SPP requests that the SQL server encrypt the session using the server certificate.
Yes	Yes	n/a	No	The SQL server rejects the connection as there is no certificate to verify against.
Yes	Yes	n/a	Yes	SPP requests that the SQL server encrypt the session and verify the server certificate against the trusted CA certificates in SPP.

MySQL Server

To support SSL you must compile the MySQL server software with SSL support and correctly configure it with a CA certificate and server certificate. If there is any problem with the certificate, the MySQL server may log an error and start up without SSL support. In this case the MySQL server rejects the request to enable SSL for a session as there is no certificate to verify against and does not encrypt the session. The MySQL server listens on a single port for both types of connections.

The behavior of the MySQL server depends on the server version and configuration. In some versions of MySQL, the server enables SSL by default on all SPP client sessions once it is configured.

If the MySQL server defaults to using SSL, or requires SSL for a user, the MySQL server encrypts the session even if the SPP client does not request it. However, the SPP client cannot request to use SSL just for encryption; it can only request SSL if you have imported the correct CA certificate to SPP.

NOTE: It is possible to detect that SSL is in use from within a session by examining the session variables. That is, the SPP client can detect if a request to use SSL has not been honored and displays an error.

Table 237: MySQL Server SSL support

SPP Use SSL Encryption Option	SSL Supported on MySQL Server	Result
No	No	Unencrypted session.
No	Yes	Determined by the MySQL server. The server encrypts the session if it defaults to using SSL or requires it for this user.
Yes	No	SPP client detects this and reports a failure.
Yes	Yes	SPP requests that the MySQL server encrypt the session and verity the server certificate against the trusted CA certificate in SPP

For more information, see Preparing MySQL servers on page 620.

Sybase ASE Server

To support SSL you must correctly configure the Sybase server with a CA certificate and server certificate. The Sybase server listens on different ports for SSL and non-SSL connections, and rejects a mismatched request from a SPP client to a particular port.

The SPP client cannot request to use SSL just for encryption; it can only request SSL if you have imported the correct CA certificate to SPP.

Table 238: Sybase ASE Server SSL support

SPP Use SSL Encryption Option	Sybase Server Listening Port Uses SSL	Result
No	No	Unencrypted session.
No	Yes	The Sybase server rejects the connection attempt. NOTE: The ODBC driver cannot detect that this is an SSL error and displays a `client cannot connect` error.
Yes	No	The Sybase server rejects the session with an SSL error.

SPP Use SSL Encryption Option	Sybase Server Listening Port Uses SSL	Result
Yes	Yes	SPP requests that the Sybase server encrypt the session and verify the server certificate against the trusted CA certificates in SPP.

For more information, see Preparing Sybase (Adaptive Server Enterprise) servers on page 625.

What are the access request states

SPPuses the following access request states, which change as a request steps through the workflow process.

Table 239: Access request states

State	Description
Available	Approved requests that are ready for the requester. That is, for password or SSH key release requests, the requester can view or copy the password or SSH key. For session access requests, the requester can launch the session.
Approved	Requests that have been approved, but the check out time has not arrived.
Denied	Requests denied by the approver.
Expired	Requests for which the **Checkout Duration** has elapsed.
Pending	Requests that are waiting for approval.
Revoked	Approved requests retracted by the approver. NOTE: The approver can revoke a request between the time the requester views it and checks it back in.

What do I do when an appliance goes into quarantine

SPP appliances can end up in a quarantine state if something goes wrong while doing certain activities. The best defense against losing data or compounding problems associated with quarantined appliances is a good and recent backup. At least one appliance

in the SPP cluster should be scheduled to periodically generate a backup and send it to an archive server. For more information, see Backup and Retention on page 151.

Recovering from a quarantine state

1. Follow these steps to create a quarantine bundle from the Recovery Kiosk. For more information, see Recovery Kiosk (Serial Kiosk) on page 646.
   a. Prior to using the **Quarantine Bundle** function, set up a Windows share where the quarantine bundle is to be sent.
   b. From the Recovery Kiosk, select the **Support Bundle** option, click the right arrow, and select **Quarantine Bundle**.
   c. Enter the following information:
      - **Address**: Enter the address of the Windows share (<IP Address>\<ShareName>) where the support bundle is to be saved.
      - If the Windows share is not anonymous, enter the **User name** and **Password** or **SSH Key**.
   d. Click **Copy to Share**.
2. You can now restart the appliance. Often, a quarantine happens because the system was waiting for a response that did not return in time. Restarting the appliance allows it to retry and frequently fixes itself.
   - To restart a quarantined appliance, connect to the Recovery Kiosk for that appliance and restart it from there. Once the appliance has restarted, it will take several minutes for SPP to start.
   - If you attempt to connect to the appliance using the web client while SPP is starting, you will get notified of HTTP Error 503. Once the log in service is running you will be presented with a log in screen, but will not be able to proceed until the appliance has proceeded further. Once the appliance has booted out of the quarantine state, you will be able to log in and proceed as normal. At this time you should generate a support bundle. If the appliance remains in a quarantine state, the web client will continue to get HTTP Error 503.

     If the web client cannot display the login screen, contact One Identity Technical Support and report the result.

     > NOTE: **Clustered environment**: If the quarantined appliance was the primary appliance, use the **Failover** option to reassign the primary appliance role to a healthy member of the cluster. For more information, see Failing over to a replica by promoting it to be the new primary on page 587.

To remove a quarantined appliance from a cluster

You may want to remove a quarantined appliance from a cluster.

1. First try to unjoin the replica appliance from the cluster. For more information, see Unjoining replicas from a cluster on page 578.

2. If unjoining the appliance fails, reset the cluster to remove the appliance from the cluster. For more information, see Resetting a cluster that has lost consensus on page 593.

Considerations for a factory reset of a hardware appliance

CAUTION: Care should be taken when performing a factory reset against a physical appliance, because this operation removes all data and audit history, returning it to its original state when it first came from the factory. Performing a factory reset will NOT reset the BMC/IPMI interface or the IP address. However, the BMC/IPMI interface will need to be reenabled after the reset has completed (for more information, see Lights Out Management (BMC)). The appliance must go through configuration again as if it had just come from the factory. For more information, see Setting up Safeguard for Privileged Passwords for the first time on page 69.

In addition, performing a factory reset may change the default SSL certificate and default SSH host key.

The appliance resets to the current Long Term Support (LTS) version. For example, if the appliance is running version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, the appliance will reset down to 6.0 LTS and you will have to patch up to your desired version. For more information, see Long Term Support (LTS) and Feature Releases on page 42.

One Identity Technical Support can determine if a factory reset is necessary. If a factory reset is the last option, you will need to contact Support to complete the operation.

1. To perform a factory reset, connect to the Recovery Kiosk and select the **Factory Reset** option. For more information, see Factory reset from the Recovery Kiosk on page 651.

   Once the factory reset is started, you must wait until it finishes (it could take up to 30 minutes to complete). When the factory reset is complete, the kiosk will return an Online indicator.

2. Once the factory reset is complete:
   a. Re-configure the network interface settings.
   b. Patch to your desired SPP version using the required patching path.
   c. If this appliance will be the primary for the cluster, upload and restore the most recent backup. For more information, see Restore a backup on page 166.
   d. If this appliance will be a replica in a cluster, there is no need to restore a backup. Join the appliance to your cluster. For more information, see Enrolling replicas into a cluster on page 577.SPP will take care of replicating all the data back to the appliance.

When does the rules engine run for dynamic grouping and tagging

Dynamic account groups are associated with rules engines that run when pertinent objects are created or changed. For example:

- Whenever you add or change an asset account, all applicable rules are reevaluated against that asset account.
- Whenever you change an asset account rule, the rule is reevaluated against all asset accounts within the scope of that rule. In other words, the rule is reevaluated against all asset accounts for grouping and the asset accounts within the designated partitions for tagging.

You can create a dynamic account group without any rules; however, no accounts will be added to this dynamic account group until you have added a rule.

In large environments, there is a possibility that the user interface may return before all of the rules have been reevaluated and you may not see the results you were expecting. If this happens, wait a few minutes and **Refresh** the screen to view the results.

Related topic:

Adding a dynamic account group

Why did the password or SSH key change during an open request

There are three ways a password or SSH key can change while a user has it checked out.

1. An Asset Administrator manually changes the password or SSH key. See: Checking, changing, or setting an account password or Checking, changing, or setting an SSH key.
2. A profile was scheduled to automatically change the password or SSH key. See: Change Password or Change SSH Key settings.
3. A policy allows both simultaneous access and requires that the password or SSH key change when a user checks it in.

If the password or SSH key changes while a user has it checked out, and the current request is still valid, the user can select either **Copy** or **Show Password** or **Show SSH Key** again to obtain the new password.

Appendix A

Safeguard ports

SPP requires port availability for various system operations.

Port details

Safeguard network port details are in the following table.

Table 240: Safeguard ports

Use in SPP	Appliance port	Protocol	Description
	MGMT	TCP	HTTPS used for a secure first-time configuration of the appliance. The IP address is a fixed address that cannot be changed. It is available in case the primary interface becomes unavailable. Typically used: TCP/443 and IP address: 192.168.1.105
Base operation	25	TCP	SMTP: Simple Mail Transfer
Base operation	53	TCP / UDP	DNS (Domain Name Server)
Base operation	123		NTP time synchronization
Base operation	88	TCP / UDP	For communication with Active Directory, Safeguard uses port 88 (for example, Kerbos authorization against Active Directory).
Base operation: AD Asset and Account Discovery, password check and change	389	TCP / UDP	LDAP used for Active Directory Asset Discovery and Directory Accounts Discovery. The standard global catalog port, 3268 (LDAP), must be open on the firewall for every Windows global catalog server in the environment and SPP Appliance to communicate for directory

Use in SPP	Appliance port	Protocol	Description
			management tasks (for example, adding a directory account, a directory user account, or a directory user group). LDAP uses port 389 for unencrypted connections. For more information, see the Microsoft publication How the Global Catalog Works. For basic functionality when changing an OS account password, the following ports are required: • Windows Active Directory: TCP/389 and TCP/445 • Windows, Windows Desktop: TCP/445 Also see: • Adding identity and authentication providers • Preparing Windows systems • Port 445
Base operation (password and SSH key check and change)	445	TCP SMB	NetLogon Service (NP-In) is used to perform: • Password check and changes for Windows Active Directory • Password and SSH key check and changes for Windows, Windows Desktop. Also see port 389 and Preparing Windows systems
LDAPS	636		Supported for non-AD LDAP providers. The default LDAPS port is 636. Port 636 needs to be open to use LDAPS for non-AD LDAP providers.
WMI	135 (49152-65535 Windows)	TCP	The firewall must be configured to allow Windows Management Instrumentation (WMI) for computer name and other lookups. WMI is also required if SPP performs any of the functions listed below on any Windows machine

Use in SPP	Appliance port	Protocol	Description
			(whether it be a dependent system or a normal target platform): • Managing service account passwords • Managing scheduled task passwords • Restarting a service • Using Account Discovery on the target WMI / DCOM from DPA will need access to TCP/135 to initiate communication on the target. The conversation continues on a random negotiated port. On Windows 7 and Windows 2008 (and above) this is in the range: 49152 - 65535. To limit the ports used by WMI/DCOM, refer to these Microsoft articles: • How to configure RPC dynamic port allocation to work with firewalls • Setting Up a Fixed Port for WMI For Windows Active Directory, if using Account Discovery or Auto Discovery CLDAP ping UDP/389 is also required. See: • Preparing Windows systems • Networking
WMI	49152-65535		See port 135

SPP/SPS internal communications	8649	TCP	Used for the SPP/SPS internal communications when SPS is linked with SPP.
			• SPS to SPP:
			  • SPS completes the link by talking to SPP on port 8649.
			  • SPS authenticates a new session and acquires the password from SPP by

Use in SPP	Appliance port	Protocol	Description
			talking on port 8649. • SPS queries SPP for cluster information and the appliance version. • SPP to SPS: • SPP queries SPS for cluster information and node roles. • SPP pushes SSH host keys to SPS when a session is initiated. • SPP queries SPS for session playback, follow mode, and session termination. In SPS, the nodes require UDP ports 500 and 4500 and TCP 8649. For the latest detail, see the *SPS Administration Guide*, Enabling cluster management.
Firewall	655	UDP (X0)	WireGuard (655) is open for secure VPN communication between appliances in a clustered high-availability configuration. To enroll an appliance into a cluster, the appliance must communicate over port 655 UDP and port 443 TCP, and must have IPv4 or IPv6 network addresses (not mixed). If both IPv4 and IPv6 are available for the connection then IPv6 will be used. See: • KB article 232289 • KB article 252260 • KB article 232671 • Cluster • Enrolling replicas into a cluster
Firewall and Client and Web browser points	443	TCP (X0)	HTTPS over TLS/SSL (443/TCP) permits inbound requests (for client/Web/API access). Used to initially log on to the appliance to join the cluster member. Users must have access to the cluster X0 ports on port 443.

Use in SPP	Appliance port	Protocol	Description
			To enroll an appliance into a cluster, the appliance must communicate over port 655 UDP and port 443 TCP, and must have IPv4 or IPv6 network addresses (not mixed). If both IPv4 and IPv6 are available for the connection then IPv6 will be used. See: • KB article 232289 • KB article 252260 • KB article 232671 • KB article 229909 (Starling related endpoint) The port is used to prepare VMware ESXi host. See: • Preparing VMware ESXi hosts
Global catalog	3268		The LDAP standard global catalog port for Active Directory. The standard global catalog port, 3268 (LDAP), must be open on the firewall for every Windows global catalog server in the environment and SPP Appliance to communicate for directory management tasks (for example, adding a directory account, a directory user account, or a directory user group). LDAP uses port 389 for unencrypted connections. For more information, see the Microsoft publication How the Global Catalog Works. Also see: • Adding an account • Adding a directory user group There are no services listening for this port on a member/server workstation (local configuration).
Kiosk	DB9	SERIAL	To connect to the Safeguard Kiosk. See KB article 233584.
Radius server	1812		Default port number that a Radius server uses to listen for authentication

Use in SPP	Appliance port	Protocol	Description
			requests. See Adding identity and authentication providers.
SonicWALL SMA or CMS appliance	8443	TCP / UDP	For SonicWALL SMA or CMS appliance. See information related to authenticating an asset, Password (local service account).
SQL server	1433		The port on which the SQL server will be listening for connections. See information related to authenticating an asset, Password (local service account).
Telnet	23	TCP	Telnet

Platform ports

ACF2 – 23

ACF2 LDAP – 389

AIX – 22

AWS – 443

Cent OS – 22

Cisco Pix – 22

Debian – 22

IDRAC – 22

ESXi - 443 default

F5 - 22 default

Fortinet – 22 default

Free BSD – 22

HP iLO

IBM i – 23

JunOS – 22

MongoDB - https://docs.mongodb.com/manual/reference/default-mongodb-port/

MySQL – 3306

Oracle – 1521

Oracle Linux – 1521

OSX – 22

Other – port is not supported for the platform

Other Managed - port is not supported for the platform

Linux – 22

Pan OS – 22

PostgreSQL – 5432 default

RACF – 23

RACF LDAP – 389

RHEL – 22

SAP Hana – 39013 default

SAP Netweaver – 3300

Solaris – 22

SoniOS – 22

SonicWall SMA – 22

SQL – 1433

SUSE – 22

SyBase – 5002

Top Secret – 23

Top Secret LDAP – 389

Ubuntu – 22

Vcenter Server – 22, 443

Windows (various depanding on OS type) – 135/389/445 and maybe dynamic ports

Archiving

Archiving uses uses SFTP/SCP and CIFS.

- SFTP/SCP: 22 TCP (X0). See the Port details table, appliance port 22 for X0.
- CIFS: Uses UDP ports 137 and 138 and TCP ports 139 and 445.

Backup

Same as Archiving.

External Authentication

Federation – Port 443

Secondary Auth – Radius Port 1812

Starling - Port 443

External Integration

SNMP – Port 162 UDP

SMTP - Port 25 TCP Simple Mail Transfer

SysLog – 514 UDP

External Integration for Password and SSH key Workflow

Cloud Assistant - 443

Ticketing – ServiceNow 443

Ticketing - Remedy 1433 (communicates to the SQL server directly)

Other

NTP – port 123 UDP

Directories – Ports 389 LDAP and 3268 global catalog

Appendix B

SPP and Safeguard for Privileged Sessions appliance link guidance

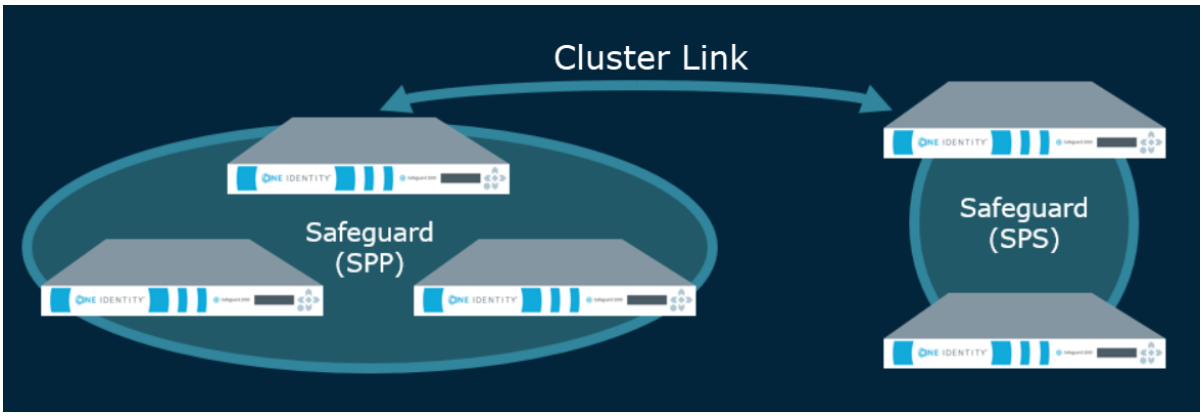
The Asset Administrator can link a Safeguard for Privileged Sessions (SPS) cluster to a SPP (SPP) cluster of one appliance or more for session recording and auditing. The actual link must be between the SPP primary and the Safeguard for Privileged Sessions cluster master. This means that the Safeguard for Privileged Sessions cluster is aware of each node in an SPP cluster and vice-versa.

Once linked, all sessions are initiated by the SPP appliance via an access request and managed by the Safeguard for Privileged Sessions appliance and sessions are recorded via the Sessions Appliance.

CAUTION: When linking your Safeguard for Privileged Sessions (SPS) deployment to your SPP (SPP) deployment, ensure that the SPS and SPP versions match exactly, and keep the versions synchronized during an upgrade. For example, you can only link SPS version 6.6 to SPP version 6.6, and if you upgrade SPS to version 6.7, you must also upgrade SPP to 6.7.

Make sure that you do not mix Long Term Supported (LTS) and feature releases. For example, do not link an SPS version 6.0.1 to an SPP version 6.1.

NOTE: If you have a single node Safeguard for Privileged Sessions cluster where the Central Management node is also the Search Master, SPP will be unable to launch sessions. There has to be at least one Safeguard for Privileged Sessions appliance in the cluster that is capable of recording sessions. See the *One Identity Safeguard for Privileged Sessions Administration Guide*, Managing Safeguard for Privileged Sessions (SPS) clusters.



Additional overview information can be found in the *One Identity Safeguard for Privileged Sessions Administration Guide*, *Using SPS with SPP*.

NOTE: Configuration options and details related to Safeguard for Privileged Sessions will only be visible to customers that have purchased and joined the product to One Identity Safeguard for Privileged Passwords.

Session recording, playback, and storage after the link

- Sessions recorded after the link are playable through SPP and are stored on the Safeguard for Privileged Sessions appliance. An archive server can be set up through Safeguard for Privileged Sessions.

Functionality after the link

The following functionality handled in SPP's user interface is available in Safeguard for Privileged Sessions after the link.

- Session certificate assignment is handled by Safeguard for Privileged Sessions. The certificate is available for audit by the Auditor.
- The primary provider names must match for a Safeguard for Privileged Sessions initiated RDP connection with SPP. See KB article 311852.

The following functionality is available in SPP after the link.

- During the link, SPP sets the **SPS Connection Policy** to `safeguard_default` for SSH or `safeguard_rdp` for RDP, as appropriate and may need to be changed. This default is nothing more than SSH or RDP connection policy.
- Other configuration set via the **Access Request Policies** dialog, are not affected by the link. These include: **General**, **Scope**, **Security**, and **Workflow** tabs.
- The Activity Center shows all old sessions and new sessions per the configuration. You can play back a session from SPP. Starting with session player 1.9.4, sessions can be played in SPP with full indexing (which makes the privileged users' activity searchable). However, if you are using an earlier version of the sessions player then indexing is only available in Safeguard for Privileged Sessions.

- Entitlement reports have not changed.
- On the Dashboard, administrators can still view and manage access requests and accounts failing tasks as usual.
- When integrating with Safeguard for Privileged Sessions, you can effectively enable Single Sign-On (SSO) between the two applications by creating and using the same SAML2 external federation login provider in both. The **Login Provider ID** value from SPP (for more information, see Identity and Authentication) must then be entered into the Safeguard for Privileged Sessions **Script Reference** field when creating the matching SAML2 login method.

Step 1: Link Safeguard for Privileged Sessions and SPP

The link is initiated from Safeguard for Privileged Sessions. For details about the link steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide*.

NOTE: SPP can target a specific Safeguard for Privileged Sessions appliance or network interface by IP address. This is done by configuring the Safeguard for Privileged Sessions connection policy to specify an explicit TO address (for example, CIDR notation /32). When that connection policy is selected as the Safeguard for Privileged Sessions connection policy for the access policy, SPP will construct a connection string that targets that specific IP address.

Pay attention to the roles assigned to the Safeguard for Privileged Sessions nodes. The following caution is offered to avoid losing session playback from SPP.

CAUTION: Do not switch the role of a Safeguard for Privileged Sessions node from the Search Local role to Search Minion role. If you do, playback of the sessions recorded while in the Search Local role may not be played back from the SPP appliance, and may only be played back via the Safeguard for Privileged Sessions web user interface. Recordings made with the node in Search Minion role are pushed to the Search Master node and are available for download to SPP. For details about Safeguard for Privileged Sessions nodes and roles, see the *One Identity Safeguard for Privileged Sessions Administration Guide*: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Step 2: Perform post link activities in SPP and Safeguard for Privileged Sessions

Steps to perform in SPP

1. The Appliance Administrator assigns the managed networks for sessions management.

   Navigate to **Appliance** > **Cluster** > **Managed Networks**. For more information, see Managed Networks on page 201.

2. The Appliance Administrator can view, delete, or edit link connections, as needed.

Go to **Appliance** > **Cluster** > **Session Appliances**. For more information, see Session Appliances with Safeguard for Privileged Sessions link on page 208.

If you soft delete a session connection, then reconnect, the access policies remain available. If you hard delete, the Security Policy Administrator will need to relink and reestablish the Safeguard for Privileged Sessions Connection Policy. For more information, see Connection deletion: soft delete versus hard delete.

3. The Security Policy Administrator identifies the session settings on the entitlements access request policy.

   Perform the following steps to ensure each policy's session setting is correctly assigned.

   a. Navigate to **Security Policy Management** > **Entitlements**, select an entitlement, and open **Access Request Policies**.
   b. Double-click a policy, or select a policy and click **Edit Access Policy**.
   c. On the **Security** tab, go to the **SPS Connection Policy**. The host name of the cluster master is displayed first followed by the IP address: `safeguard_default`.
   d. If needed, select the cluster or appliance to which the policy applies.

      For more information, see Session Settings tab on page 1.

4. While on the **Access Request Policies** dialog, the Security Policy Administrator checks any other tab, as needed. The link does not affect the settings on the tabs including the **General**, **Scope**, **Security**, and **Workflow** tabs.

Steps to perform in Safeguard for Privileged Sessions

Complete any set up in Safeguard for Privileged Sessions required (such as setting up an archive server, the SSH banner, the SSH host key, as well as SSH-related or RDP-related command detection and controls). For details, see the *One Identity Safeguard for Privileged Sessions Administration Guide*: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Standard operating procedure after the initial link

If you add another Safeguard for Privileged Sessions (SPS) cluster after the initial link, follow these standard operating procedures:

1. Add link connections. For more information, see Session Appliances with Safeguard for Privileged Sessions link on page 208.
2. Identify the session settings on the entitlements access request policy (**SPS Connection Policy** that is the IP address of the cluster master). For more information, see Creating an access request policy.
3. Assign the managed networks. For more information, see Managed Networks.

Appendix C

Regular expressions

Regular expressions are used to parse large amounts of data to find matching patterns and validate a predefined pattern. For example, in SPP, regular expressions are used for:

- Account Discovery rules (Property Constraints, Name Ranges and Group Ranges). Partial matches are acceptable (unless the regular expression itself is defined to only return exact matches).
- Ticket numbers when an external ticketing system is not used. Matches must be exact.

For details, see these Microsoft resources:

- .NET Regular Expressions
- Regular Expression Language - Quick Reference

Best practices for ticketing not tied to external ticket system

These best practices are for adding a regular expression for ticketing not tied to an external ticket system. For more information, see Ticket systems on page 238.

If you use an alternation construct ("|" which is "or"), the longest matching expression is defined first to the least matching expression because Windows.Net regular expression (regex) stops after finding the first match.

For example: `A{3}[0-9]{5}ZZZ|A{3}[0-9]{5}` is advised instead of the reverse order. Sample entry results follow for the `A{3}[0-9]{5}ZZZ|A{3}[0-9]{5}` expression:

User entry:	Match?
AAA12345	Yes. Matched on the second regex
AAA12345Z	No. There is no exact match.
AAA12345ZZZ	Yes. Matched on the first regex. If the expression were reversed (`A{3}[0-9]{5}|A{3}[0-9]{5}ZZZ`) there would be a partial match on the first expression and the entry would be returned as invalid.

You may want to wrap each expression in an alternation construct with the anchors `^` and `$` when using alternation constructs. An example follows: `^A{3}[0-9]{5}ZZZ$|^A{3}[0-9]{5}$`.

The `?` lazy quantifier should be avoided, especially at the end of the expression. For example, if the regex is `A{3}[0-9]?` and the user enters `AAA12345`, `AAA1` is returned as a matched string which is not an exact match of `AAA12345`.

If the greedy quantifier (`*`) is used against `AAA12345` then the matched string will be `AAA12345` and be an exact match.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to videos at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product