Safeguard for Privileged Passwords 6.0.7 LTS

Administration Guide

Copyright 2020 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. 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.

Safeguard for Privileged Passwords Administration Guide
Updated - 28 August 2020, 01:41
Version - 6.0.7 LTS

Contents

Introduction **19**
Introduction to Safeguard for Privileged Passwords 19
Overview of the entities 21
Key features 27
Appliance specifications 31
System requirements and versions **34**
Desktop client system requirements 35
Web client system requirements 36
Web management console system requirements 37
Supported platforms 37
Setting up the virtual appliance 42
License: hardware, virtual, expiration 45
Long Term Support (LTS) and Feature Releases 46
Using API and PowerShell tools **49**
Using the API 49
Access the SPP API 49
Customize the response using API query parameters 52
Safeguard PowerShell 53
Using the virtual appliance and web management console **55**
Virtual appliance backup and recovery 57
Support Kiosk 58
Cloud deployment considerations **61**
Before you start: platforms and resources 61
Restricting access to the web management kiosk for cloud deployments 61
AWS deployment 63
Azure deployment 64
Virtual appliance backup and recovery 66
Setting up Safeguard for Privileged Passwords for the first time **68**
Step 1: Create the Authorizer Administrator 68
Step 2: Authorizer Administrator creates administrators 69

Step 3: Appliance Administrator configures the appliance 69
Step 4: User Administrator adds users 70
Step 5: Asset Administrator adds managed systems 71
Step 6: Security Policy Administrator adds access request policies 71

Using the web client 72
Home 72
My Requests (web client) 74
Approvals (web client) 75
Reviews (web client) 76
Favorites (web client) 76
Settings, version, and desktop Windows client (web client) 77
Change password (web client) 78
FIDO2 keys (web client) 79
Log out (web client) 79

Getting started with the desktop client 80
Installing the desktop client 80
Starting the desktop client 82
Uninstalling the desktop client 83

Using the desktop client 84
Settings (desktop client) 84
User information and log out (desktop client) 86
Desktop client favorite request 88
Desktop client navigation pane 89
Home 90
Dashboard 92
Access Requests 92
Account Automation 93
Activity Center 94
Applying search criteria 95
Saving search criteria 97
Generating an activity audit log report 97
Scheduling an activity audit log report 99
Editing or deleting a saved search or scheduled report 101
Viewing event details 102

Auditing request workflow 102
Filtering report results 103
Sorting report results 103
Reports 104
Running an entitlement report 105
Converting time stamps 106
Administrative Tools 107
Toolbar options 109

Search box 111
Search by attribute 112
Select a drop-down to sort 114

Privileged access requests 117
Configuring alerts 118
Toast notifications 118
Email notifications 118
Password release request workflow 120
Requesting a password release 121
Taking action on a password release request 123
Approving a password release request 125
Reviewing a completed password release request 127
Session request workflow 128
About sessions and recordings 128
Requesting session access 129
Taking action on a session request 133
Approving a session request 137
Launching the SSH client 138
Launching an RDP session 139
Reviewing a session request 141
Replaying a session 142
Following and terminating a "live" session 143

Toolbox 145
Viewing task status 145
Stopping a task 146

Accounts 147

General tab (account) 148
Access Request Policies tab (account) 150
Account Groups tab (account) 151
Dependent Assets (account) 152
Check and Change Log tab (account) 153
History tab (account) 154
Managing accounts 155
Adding an account 156
Adding a cloud platform account 157
Manually adding a tag to an account 159
Adding an account to one or more account groups 159
Modifying an account 160
Deleting an account 160
Importing objects 161
Creating an import file 164
Checking, changing, or setting an account password 165
Viewing password archive 166

Account Groups 167
General tab (account group) 168
Accounts tab (account group) 168
Access Request Policies tab (account group) 169
History tab (account group) 170
Managing account groups 172
Adding an account group 172
Adding a dynamic account group 172
General tab (add dynamic account group) 173
Account Rules tab (add dynamic account group) 174
Summary tab (add dynamic account group) 176
Adding one or more accounts to an account group 176
Adding accounts to an access request policy 177
Modifying an account group 177
Deleting an account group 177

Assets 179
General tab (asset) 182

Accounts tab (asset) 186
Account Dependencies tab (asset) 188
Access Request Policies tab (asset) 188
Asset Groups tab (asset) 189
Discovered Services tab (asset) 190
History tab (asset) 191
Managing assets 192
Adding an asset 193
General tab (add asset) 194
Management tab (add asset) 195
Account Discovery tab (add asset) 198
Connection tab (add asset) 200
Attributes tab (add asset) 211
Checking an asset's connectivity 212
Assigning an asset to a partition 213
Assigning a profile to an asset 213
Manually adding a tag to an asset 214
Adding an account to an asset 215
Adding account dependencies 216
Adding an asset to asset groups 218
Modifying an asset 218
Deleting an asset 219
Importing objects 219
Downloading a public SSH key 222

Asset Groups 223
General tab (asset group) 224
Assets tab (asset group) 224
Access Request Policies tab (asset group) 225
History tab (asset group) 226
Managing asset groups 227
Adding an asset group 227
Adding a dynamic asset group 228
General tab (add dynamic asset group) 229
Asset Rules tab (add dynamic asset group) 229
Summary tab (add dynamic asset group) 231

Adding assets to an asset group 231
Modifying an asset group 232
Deleting an asset group 232

Discovery 233
Asset Discovery 234
Asset Discovery job workflow 236
Adding an Asset Discovery job 236
General tab (asset discovery) 237
Information tab (asset discovery) 238
Rules tab (asset discovery) 239
Schedule tab (asset discovery) 245
Summary tab (asset discovery) 246
Editing an Asset Discovery job 246
Deleting an Asset Discovery job 247
Asset Discovery Results 247
Account Discovery 248
Account Discovery job workflow 251
Adding an Account Discovery job 251
Adding an Account Discovery rule 254
Editing an Account Discovery job 258
Deleting an Account Discovery job 259
Account Discovery Results 259
Discovered Accounts 260
Service Discovery Results 261
Discovered Services 262

Entitlements 266
General tab 267
Users tab 268
Access Request Policies tab 269
History tab 271
Managing entitlements 273
Adding an entitlement 273
General tab 273
Time Restrictions tab 275

Creating an access request policy ... 276
General tab ... 277
Scope tab ... 278
Requester tab ... 279
Approver tab ... 280
Reviewer tab ... 282
Access Config tab ... 284
Session Settings tab ... 285
Time Restrictions tab ... 286
Emergency tab ... 286
Adding users or user groups to an entitlement ... 287
Deleting an access request policy ... 288
Modifying an access request policy ... 289
Copying an access request policy ... 289
Viewing and editing policy details ... 289
Modifying an entitlement ... 290
Deleting an entitlement ... 290

Partitions ... 292
About partition profiles ... 293
General tab (partitions) ... 294
Assets tab (partitions) ... 295
Accounts tab (partitions) ... 296
Profiles tab (partitions) ... 297
History tab (partitions) ... 298
Managing partitions ... 300
Adding a partition ... 300
Adding assets to a partition ... 301
Removing assets from a partition ... 302
Creating a profile ... 302
Modifying a profile ... 303
Setting a default partition ... 304
Setting a default partition profile ... 305
Assigning assets or accounts to a profile ... 305
Modifying a partition ... 306
Deleting a partition ... 307

Settings **308**
Access Request settings 309
Enable or Disable Services (Access and management services) 309
Reasons 312
Appliance settings 313
Appliance Diagnostics 314
Appliance Information 315
Setting the appliance name 317
Shutting down the appliance 318
Restarting the appliance 319
Enable or Disable Services 319
Factory Reset from the desktop client 320
Licensing 321
Lights Out Management (BMC) 322
Network Diagnostics 323
Ping 323
NS Lookup 324
Trace Route 325
Telnet 325
Show Routes 326
Networking 326
Operating system licensing 329
Support bundle 330
Time 330
Updates 331
Asset Management settings 332
Custom platforms 333
Creating a custom platform script 334
Adding a custom platform 335
Tags 335
Adding a tag for dynamic tagging of assets or asset accounts 337
Deleting an asset or asset account tag 341
Modifying an asset or asset account tag 341
Copying an asset or asset account tag to another partition 342
Viewing asset and asset account tag assignments 342

Backup and Retention settings ... 343
About backups ... 343
Archive servers ... 344
Adding an archive server ... 345
Audit Log Management ... 346
Backup and restore ... 348
Run Now ... 350
Backup settings ... 350
Download ... 352
Upload ... 352
Restore ... 353
Archive backup ... 354
Backup retention ... 354
Certificate settings ... 355
About certificates ... 355
Audit Log Signing Certificate ... 356
Installing an audit log signing certificate ... 358
Creating a Certificate Signing Request for audit logs ... 359
Certificate Signing Request ... 359
SSL Certificates ... 360
Installing an SSL certificate ... 362
Creating a Certificate Signing Request ... 362
Assigning a certificate to appliances ... 363
Trusted Certificates ... 363
Adding a trusted certificate ... 364
Removing a trusted certificate ... 364
Cluster settings ... 365
Cluster Management ... 366
Cluster view pane ... 367
Appliance details and cluster health pane ... 367
Managed networks ... 369
Adding a managed network ... 373
Deleting a managed network ... 374
Resolving IP address ... 374
Offline Workflow (automatic) ... 374

Enable automatic Offline Workflow 375
Manually override automatic Offline Workflow 376
Session Appliances with SPS join 377
External Integration settings 381
Application to Application 382
About Application to Application functionality 383
Setting up Application to Application 385
Adding an application registration 386
Deleting an application registration 388
Regenerating an API key 388
Making a request using the Application to Application service 388
Approval Anywhere 393
Adding authorized user for Approval Anywhere 394
Email 395
Enabling email notifications 396
Modifying an email template 397
Identity and Authentication 398
Authentication provider combinations 399
Adding identity and authentication providers 402
SNMP 410
Configuring SNMP subscriptions 411
Verifying SNMP configuration 412
Starling 412
Join Starling 412
Syslog 415
Configuring a syslog server 416
Verifying syslog server configuration 417
Ticketing systems 417
Messaging settings 420
Login Notification 420
Message of the Day 420
Profile settings 421
Account Password Rules 421
Adding an account password rule 422
Change Password 425

Adding change password settings 426
Check Password 429
Adding check password settings 430
Password sync groups 432
Adding a password sync group 433
Modifying a password sync group 434
Safeguard Access settings 435
Login Control 436
Password Rule 438
Modifying user password requirements 439
Time Zone 442
Users 443
General tab (user) 444
User Groups tab (user) 446
Partitions tab (user) 446
Entitlements tab (user) 447
Linked Accounts tab (user) 448
History (user) 450
Managing users 451
Adding a user 451
Identity tab (add user) 452
Authentication tab (add user) 453
Location tab (add user) 455
Permissions tab (add user) 456
Requiring secondary authentication log in 457
Configuring user for Starling Two-Factor Authentication when logging in to Safeguard 458
Adding a user to user groups 459
Assigning a user to partitions 459
Adding a user to entitlements 459
Linking a directory account to a user 460
Modifying a user 461
Enabling or disabling a user 461
Deleting a user 462
Importing objects 462

Setting a local user's password 465
Unlocking a user's account 466

User Groups 467
General tab (user groups) 468
Users tab (user groups) 468
Entitlements tab (user groups) 469
History tab (user groups) 471
Managing user groups 472
Adding a user group 472
Adding a directory user group 473
Adding users to a user group 476
Adding a user group to an entitlement 477
Modifying a user group 477
Deleting a user group 478

Disaster recovery and clusters 479
Enrolling replicas into a cluster 482
Considerations to enroll cluster members 482
Unjoining replicas from a cluster 483
Considerations to unjoin cluster members 484
Maintaining and diagnosing cluster members 485
About Offline Workflow Mode 486
Manually control Offline Workflow Mode 489
Failing over to a replica by promoting it to be the new primary 491
Activating a read-only appliance 492
Diagnosing a cluster member 492
Patching cluster members 493
About cluster patching 494
Using a backup to restore a clustered appliance 495
Resetting a cluster that has lost consensus 497
Performing a factory reset 498
Unlocking a locked cluster 501
Troubleshooting tips 501
Appliance states 502

Administrator permissions 507

Appliance Administrator permissions 507
Asset Administrator permissions 509
Auditor permissions 511
Authorizer Administrator permissions 512
Help Desk Administrator permissions 513
Operations Administrator permissions 514
Security Policy Administrator permissions 516
User Administrator permissions 517

Preparing systems for management 519
Preparing ACF - Mainframe systems 520
Preparing Amazon Web Services platforms 521
Preparing Cisco devices 521
Preparing Dell iDRAC devices 522
Preparing VMware ESXi hosts 522
Preparing Fortinet FortiOS devices 523
Preparing F5 Big-IP devices 523
Preparing HP iLO servers 524
Preparing HP iLO MP (Management Processors) 524
Preparing IBM i (AS/400) systems 524
Preparing JunOS Juniper Networks systems 525
Preparing MongoDB 526
Preparing MySQL servers 526
Preparing Oracle databases 527
Preparing PAN-OS (Palo Alto) networks 527
Preparing PostgreSQL 527
Preparing RACF mainframe systems 528
Preparing SAP HANA 529
Preparing SAP Netweaver Application Servers 529
Preparing Sybase (Adaptive Server Enterprise) servers 530
Preparing SonicOS devices 531
Preparing SonicWALL SMA or CMS appliances 531
Preparing SQL Servers 531
Preparing Top Secret mainframe systems 533
Preparing Unix-based systems 534
Preparing Windows systems 535

Minimum required permissions for Windows assets 536
Preparing Windows SSH systems 538

Troubleshooting 539
Anti-CSRF (cross-site request forgery) token error 540
Connectivity failures 540
Change password fails 540
Incorrect authentication credentials 541
Missing or incorrect SSH host key 541
No cipher supported error 542
Service account has insufficient privileges 542
Cannot connect to remote machine through SSH or RDP 543
Cannot delete account 543
Cannot play session message 544
Domain user denied access to Safeguard for Privileged Passwords 544
LCD status messages 544
Appliance LCD and controls 545
My Mac keychain password was lost 546
Password fails for Unix host 547
Password is pending review 547
Password is pending a reset 548
Profile did not run 548
Recovery Kiosk (Serial Kiosk) 549
Appliance information (Recovery Kiosk) 550
Power options 551
Rebooting the appliance 551
Shutting down the appliance 552
Admin password reset 552
Factory reset from the Recovery Kiosk 553
Support bundle 554
Replica not adding 554
System services did not update or restart after password change 555
Test Connection failures 555
Test Connection failures on archive server 556
Certificate issue 556
Cipher support 556

Domain controller issue 557
Networking issue 558
Windows WMI connection 558
Timeout errors causing operations to fail 558
User locked out 559
User not notified 559

Frequently asked questions 560
How do I audit transaction activity 560
How do I configure external federation authentication 561
How do I add an external federation provider trust 562
How do I create a relying party trust for the STS 563
How do I add an external federation user account 564
How do I manage accounts on unsupported platforms 564
How do I modify the appliance configuration settings 566
How do I prevent Safeguard for Privileged Passwords messages when making RDP connections 567
How do I set up telnet and TN3270/TN5250 session access requests 569
How do I set the appliance system time 571
How do Safeguard for Privileged Passwords database servers use SSL 571
ODBC Transport 572
Microsoft SQL Server 572
MySQL Server 573
Sybase ASE Server 574
What are the access request states 575
What do I do when an appliance goes into quarantine 575
When does the rules engine run for dynamic grouping and tagging 577
Verifying syslog server configuration 578
Why did the password change during an open request 578

Appendix: Safeguard ports 580

Appendix: SPP 2.7 or later migration guidance 587

Appendix: SPP and SPS sessions appliance join guidance 592

Appendix: Regular expressions 597

SPP glossary 599

About us **616**
Contacting us 616
Technical support resources 616
Index **617**

1

Introduction

The 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 Safeguard for Privileged Passwords for the first time.

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

Introduction to Safeguard for Privileged Passwords

The Safeguard for Privileged Passwords Appliance is built specifically for use only with the Safeguard for Privileged Passwords 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.

Safeguard for Privileged Passwords 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:

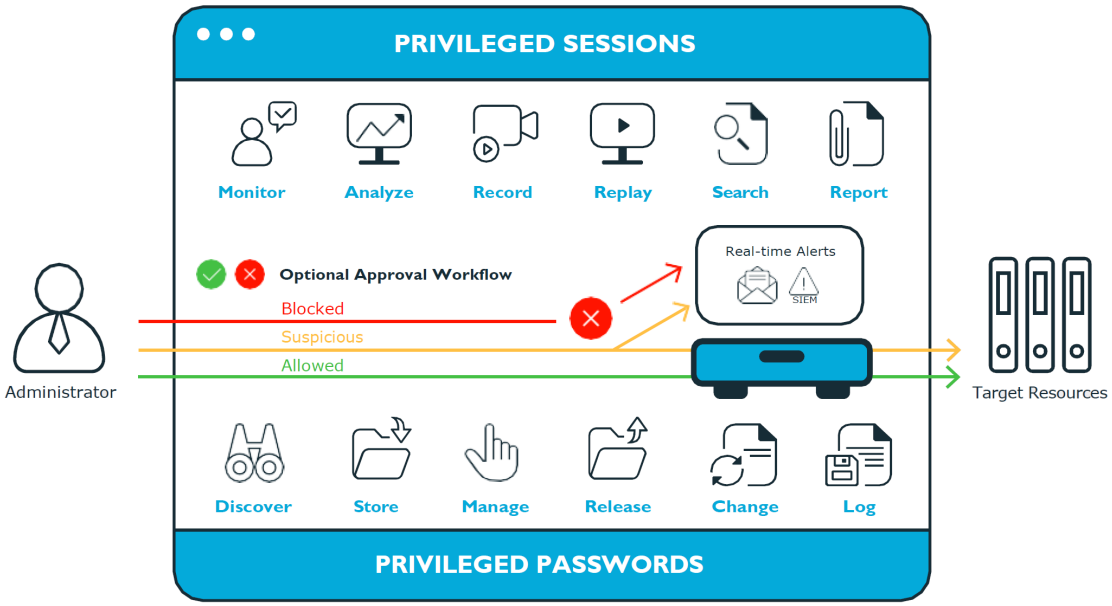
- One-stop solution for all privileged access management needs
- Easy to deploy and integrate
- Unparalleled depth of recording
- Comprehensive risk analysis of entitlements and activities
- Thorough Governance for privileged account

The suite includes the following modules:

- **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, Safeguard for Privileged Passwords 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.
- **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 partition 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 (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 partition profile includes the schedules and rules governing the partition’s assigned assets and the assets' accounts. For example, the partition profile defines how often a password check is required on an asset or account.

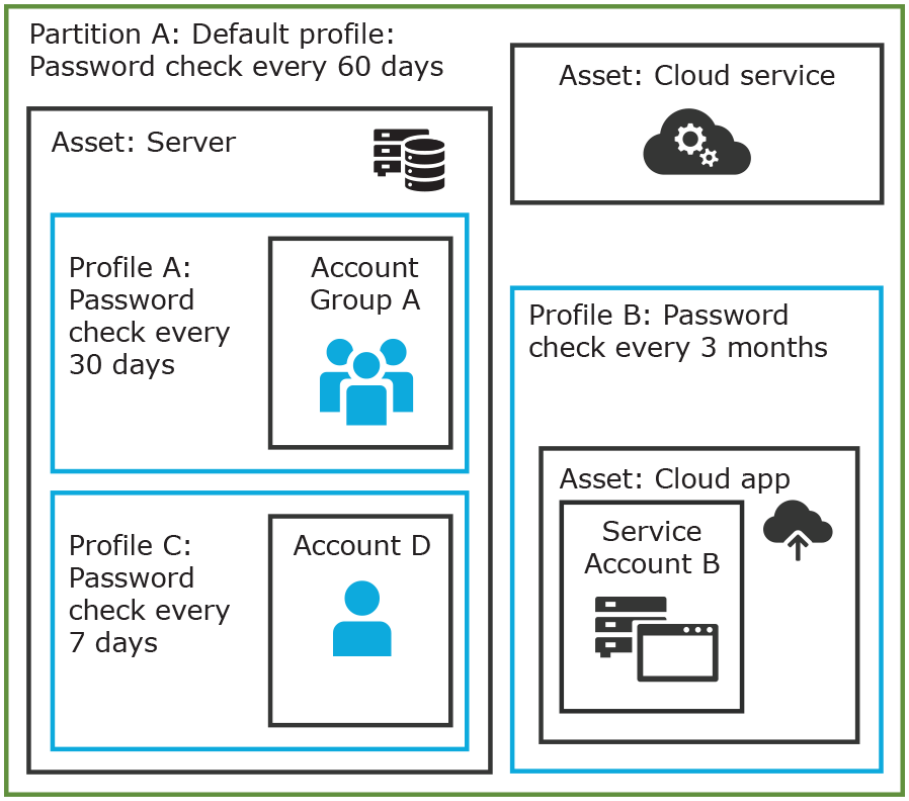
A partition can have multiple partition profiles, each assigned to different assets, if desired. An account is governed by only one profile. If an account is not explicitly assigned to a profile, the account is governed by the one assigned to the parent asset. If that asset does not have an assigned 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. For more information, see Adding change password settings.

When you create a new partition, Safeguard for Privileged Passwords 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 partition 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, Safeguard for Privileged Passwords 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 partition 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 partition profiles

- A partition is a group of assets (and the assets' associated accounts) governed by a partition 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.

- Partition profiles are the schedules and rules that govern a partition's assets and the assets' accounts. You can set a default partition profile to assign or you can manually assign a partition 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 includes password and sessions.

- To define an access request policy for a password 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**. For more information, see Access Config tab on page 284.

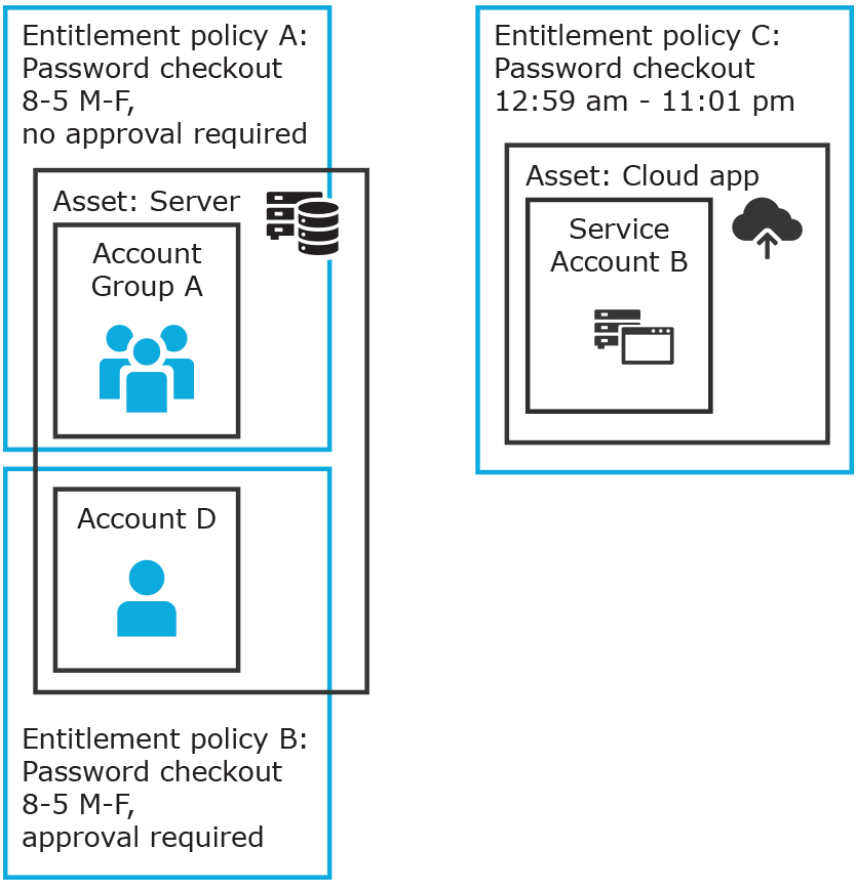
Entitlement access request policies may include:

- The access type: Password or sessions which can include the protocols Secure SHell (SSH), Remote Desktop Protocol (RDP), or 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, ththis includes the approvers and reviewers along with notifications
- Access configuration: Settings based on the type of access (Password, SSH client, 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 Safeguard for Privileged Passwords. 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 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 Safeguard for Privileged Passwords.
- 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.

Key features

The One Identity portfolio includes the industry's most comprehensive set of privileged access management solutions. You can build on the capabilities of One Identity Safeguard with solutions for granular delegation of the Unix root account and the Active Directory administrator account; add-ons to make open source sudo enterprise-ready; and keystroke logging for Unix root activities – all tightly integrated with the industry's leading Active Directory bridge solution.

The following key features are available in Safeguard for Privileged Passwords.

Feature information by release is available. For more information, see Appendix D: Historical changes by release.

Table 1: One Identity Safeguard for Privileged Passwords key features

Feature	Description
Auto-login	Auto-login and sessions access request launch enhances security and compliance by never exposing the account credentials to the user.
Activity Center	Using the Activity Center, you can quickly and easily view all actions executed by Safeguard for Privileged Passwords users and integrated processes. Activity Center reports can be searched, customized, and filtered to zero in on the actions of a single user or to audit a variety of actions across a subset of departments. In addition, you can schedule queries, and save or export the data.
Always online	Safeguard for Privileged Passwords Appliances can be clustered to ensure high availability. Passwords and sessions can be requested

Feature	Description
	from any appliance in a Safeguard for Privileged Passwords cluster. This distributed clustering design also enables the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
Approval Anywhere	Leveraging One Identity Starling, you can approve or deny any access request anywhere without being on the VPN.
Cloud support	Safeguard for Privileged Passwordscan be run in the cloud using Azure or AWS.

Directory integration	You can leverage your existing directory infrastructure (such as Microsoft Active Directory). You import directory users and directory groups. Directory users authenticate to Safeguard for Privileged Passwords with their directory credentials. Managed account users cannot be members of the Protected Users AD Security Group.
	Active Directory and LDAP data is automatically synchronized by asset or identity and authentication providers schema as shown in the following lists.
	Asset schema list
	• Users
	  • Username
	  • Password (modifiable in LDAP and not modifiable in Active Directory)
	  • Description
	• Groups
	  • Name
	  • Member
	• Computer
	  • Name
	  • Network Address
	  • Operating System
	  • Operating System Version
	  • Description
	Identity and Authentication Providers schema list
	• Users
	  • Username

Feature	Description
	• First Name • Last Name • Work Phone • Mobile Phone • Email • Description • External Federation Authentication • Radius Authentication • Managed Objects • Groups • Name • Members • Description
Discovery	Quickly discover any privileged account or system on your network with host , directory, and network-discovery options.
Event notification options	Safeguard for Privileged Passwords allows you to configure the appliance to send event notifications to external systems such as Email, Syslog, and SNMP.
Favorites	Quickly access the passwords that you use the most right from the Home screen. You can group several password requests into a single favorite so you can get access to all the accounts you need with a single click.
One Identity Hybrid Subscription	Expand the capabilities of Safeguard with the One Identity Hybrid Subscription, which offers immediate access to cloud delivered features and services. These include all-you-can-eat Starling Two-Factor Authentication (2FA) to protect Safeguard access and Starling Identity Analytics & Risk Intelligence for Safeguard so that you can preemptively detect risk users and entitlements. A single subscription enables all One Identity solution deployments.
Partitions and Profiles	Safeguard for Privileged Passwords allows you to group managed systems into secure work areas that can be designated for delegated management.
Release control	Manages password requests from authorized users for the accounts they are entitled to access via a secure web browser connection with support for mobile devices.
RESTful API	Safeguard for Privileged Passwords (SPP) is built with an API-first

Feature	Description
	design and uses a modernized API based on a REST architecture that allows other applications and systems. Every function is exposed through the API to enable quick and easy integration regardless of what you want to do or which language your applications are written in. There are even a few things that can only only be done via the Safeguard SPP API. The Safeguard for Privileged Passwords API tutorial is available on GitHub at: https://github.com/oneidentity/safeguard-api-tutorial.
Role-based access control (RBAC)	Safeguard for Privileged Passwords uses a role-based access control hierarchy using administrator permissions sets. Numerous roles are available for administrating Safeguard for Privileged Passwords, enabling granular delegation and workflows along with least privileged access.
Secure access to legacy systems	Use smartcard, two-factor authentication, or other strong authentication methods to gain access to systems. Because Safeguard for Privileged Passwords acts as a gateway or proxy to the system, it enables strong authentication to targets that cannot or do not support those methods natively.
Smartcard support	Authentication of your privileged users can be integrated with Microsoft's Active Directory support for Smartcards or manually uploaded to the Safeguard for Privileged Passwords Appliance itself.
Two-factor authentication support	Protecting access to passwords with another password isn't enough. Enhanced security by requiring two-factor authentication to Safeguard for Privileged Passwords. Safeguard for Privileged Passwords supports any Radius-based 2FA solution and One Identity's Starling Two-Factor Authentication (2FA) service.
Workflow engine for policy-based release control	Using a secure web browser with support for mobile devices, you can request access and provide approval for privileged passwords and sessions. Requests can be approved automatically or require dual/multiple approvals based on your organization’s policy. The workflow engine supports time restrictions, multiple approvers and reviewers, emergency access, and expiration of policy. It also includes the ability to input reason codes and/or integrate directly with ticketing systems or tickets used for internal tracking only.

Sessions key features

To record and playback sessions, use Safeguard for Privileged Sessions via a join to Safeguard for Privileged Passwords.

The join is initiated from Safeguard for Privileged Sessions. For details about the join steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide*.

For more information, see SPP and SPS sessions appliance join guidance.

Appliance specifications

The Safeguard for Privileged Passwords Appliance is built specifically for use only with the Safeguard for Privileged Passwords 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 two tables list the Safeguard for Privileged Passwords 3000 Appliance and 2000 Appliance specifications and power requirements.

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
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: 3000 Appliance and 2000 Appliance: Power requirements

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

Safeguard for Privileged Passwords 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

Safeguard for Privileged Passwords has several graphical user interfaces that allow you to manage access requests, approvals, and reviews for your managed accounts and systems:

- The Windows desktop client consists of an end-user view and administrator view. The fully featured desktop client exposes all of the functionality of Safeguard based on the role of the authenticated user.
- The web client is functionally similar to the desktop client end-user view and useful for requestors, reviewers, and approvers. Many administration functions are available as well.
- 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 joined to Safeguard for Privileged Passwords, session recording is handled via Safeguard for Privileged Session. The join is initiated from Safeguard for Privileged Sessions. For details about the join 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/TCP 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.

Desktop client system requirements

The desktop client is a native Windows application suitable for use on end-user machines. You install the desktop client by means of an MSI package that you can download from the appliance web client portal. You do not need administrator privileges to install Safeguard for Privileged Passwords.

NOTE: PuTTY is used to launch the SSH client for SSH session requests and is included in the install. The desktop client looks for any user-installed PuTTY in the following locations:

- Any reference to putty in the PATH environment variable
- `c:/Program Files/Putty`
- `c:/Program Files(x86)/Putty`
- `c:/Putty`

If PuTTY is not found, the desktop client uses the version of PuTTY that it installed at:

`<user-home-dir>/AppData/Local/Safeguard/putty`.

If the user later installs PuTTY in any of the locations above, the desktop client uses that version which ensures the user has the latest version of PuTTY.

Table 5: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6 (or later)
Windows platforms	64-bit editions of: • Windows 7 • Windows 8.1 • Windows 10 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 If the appliance setting, **TLS 1.2 Only** is enabled, (**Administrative Tools** | **Settings** | **Appliance** | **Appliance Information**), ensure the desktop client also has TLS 1.2 enabled. If the client has an earlier version of TLS enabled, you will be locked out of the client and will not be able to connect to Safeguard for Privileged Passwords. IMPORTANT: The Windows 7 Desktop client has additional requirements in order to enable TLS 1.2. For information, see

Component	Requirements
	Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows. Considerations: • Internet Explorer security must be set to use TLS 1.0 or higher. Ensure the proper "Use TLS" setting is enabled on the Advanced tab of the **Internet Options** dialog (In Internet Explorer, go to **Tools** | **Internet Options** | **Advanced** tab). • To use FIDO2 two-factor authentication, you will need a web browser that supports the WebAuthn standard.
Desktop Player	See *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide* available at: One Identity Safeguard for Privileged Sessions - Technical Documentation, **User Guide**.

Web client system requirements

Table 6: Web requirements

Component	Requirements
Web browsers	Desktop browsers: • Apple Safari 13.1 for desktop (or later) • Google Chrome 80 (or later) • Microsoft Edge 80 (or later) • Mozilla Firefox 69 (or later) • Microsoft Internet Explorer 11 (Newer features may not work with Internet Explorer. You are encouraged to upgrade to a browser that can support all functionality.) Mobile device browsers: • Apple iOS 13 (or later) • Google Chrome on Android version 80 (or later)

Web management console system requirements

Table 7: Web kiosk requirements

Component	Requirements
Web management console	Desktop browsers: • Apple Safari 13.1 for desktop (or later) • Google Chrome 80 (or later) • Microsoft Edge 80 (or later) • Mozilla Firefox 69 (or later) • Microsoft Internet Explorer 11 (Newer features may not work with Internet Explorer. You are encouraged to upgrade to a browser that can support all functionality.)

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) version 6.5 or higher
  - VMware Worksation 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

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

Safeguard for Privileged Passwords tested platforms

The following table lists the platforms and versions that have been tested for Safeguard for Privileged Passwords (SPP). Additional assets may be added to Safeguard for Privileged Passwords. If you do not see a particular platform listed when adding an asset, use the

Other, **Other Managed**, or **Other Linux** selection on the **Management** tab of the **Asset** dialog. For more information, see Management tab (add asset) on page 195.

SPP joined to SPS: Sessions platforms

When Safeguard for Privileged Passwords (SPP) is joined 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.

Supported platform updates

For all supported platforms, it is assumed that the latest updates are applied.

Table 8: Supported platforms: Assets that can be managed

Platform	Version	Architecture (all versions unless noted)	Supports SPP	Supports SPS Access
ACF2 - Mainframe	r14, r15	zSeries	True	True
ACF2 - Mainframe LDAP	r14, r15	zSeries	True	False
Active Directory			True	False
AIX	6.1, 7.1, 7.2	PPC	True	True
Amazon Linux	2	x86_64	True	True
Amazon Web Services (AWS)	1		True	False
CentOS Linux	6 7	(ver 6) x86, x86_64 (ver 7) x86_64	True	True
Cisco ASA	7.x, 8.x		True	True
Cisco IOS	12.X, 15.X		True	True
Debian GNU/Linux	6, 7, 8, 9	x86, x86_64, MIPS, PPC, zSeries	True	True

Platform	Version	Architecture (all versions unless noted)	Supports SPP	Supports SPS Access
Dell iDRAC	7, 8		True	True
ESXi (VSphere)	5.5, 6.0, 6.5, 6.7		True	False
F5 Big-IP	12.1.2, 13.0, 14.0		True	True
Fedora	21, 22, 23, 24, 25, 26, 27, 28, 29, 30	x86, x86_64	True	True
Fortinet FortiOS	5.2, 5.6		True	True
FreeBSD	10.4, 11.1, 11.2	x86, x86_64	True	True
HP iLO	2, 3, 4	x86	True	True
HP iLO MP	2, 3	IA-64	True	True
HP-UX	11iv2 (B.11.23), 11iv3 (B.11.31)	PA-RISC, IA-64	True	True
IBM i (formerly AS/400)	7.1, 7.2, 7.3	PPC	True	True
Junos - Juniper Networks	12, 13, 14, 15		True	True
macOS	10.9, 10.10, 10.11, 10.12, 10.13	x86_64	True	True
MongoDB	3.4, 3.6, 4.0		True	False
MySQL	5.6, 5.7		True	False
OpenLDAP	2.4		True	False
Oracle	11g Release 2, 12c Release 1		True	False
Oracle Linux (OEL)	6 7	(ver 6) x86, x86_64 (ver 7) x86_64	True	True
Other			False	False
Other Linux			True	True
Other			True	False

Platform	Version	Architecture (all versions unless noted)	Supports SPP	Supports SPS Access
Managed				
PAN-OS	6.0, 7.0, 8.0, 8.1		True	True
PostgreSQL	9.6, 10.2, 10.3, 10.4, 10.5		True	False
RACF - Mainframe	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries	True	True
RACF - Mainframe LDAP	z/OS V2.1 Security Server, z/OS V2.2 Security Server	zSeries	True	False
Red Hat Enterprise Linux (RHEL)	6, 7, 8	(ver 6) x86, x86_64, PPC, zSeries (ver 7 and 8) x86, x86_64, PPC, zSeries	True	True
SAP HANA	2.0	Other	True	False
SAP Netweaver Application Server	7.3, 7.4, 7.5		True	False
Solaris	10, 11	(ver 10) SPARC, x86, x86_64 (ver 11) SPARC, x86_64	True	True
SonicOS	5.9, 6.2		True	False
SonicWALL SMA or CMS	11.3.0		True	False
SQL Server	2012, 2014, 2016, 2017, 2019		True	False
SUSE Linux Enterprise Server (SLES)	11 12	(ver 11) x86, x86_64, PPC, zSeries, IA-64 (ver 12) x86_64, PPC, zSeries	True	True
Sybase (Adaptive Server	15.7, 16		True	False

Platform	Version	Architecture (all versions unless noted)	Supports SPP	Supports SPS Access
Enterprise)				
Top Secret - Mainframe	r14, r15	zSeries	True	True
Top Secret - Mainframe LDAP	r14, r15	zSeries	True	False
Ubuntu	14.04 LTS, 15.04, 15.10, 16.04 LTS, 16.10, 17.04, 17.10, 18.04 LTS, 18.10, 19.04	x86, x86_64	True	True
Windows	Vista, 7, 8, 8.1, 10 Enterprise (including LTSC and IoT).		True	True
Windows Server	2008, 2008 R2, 2012, 2012 R2, 2016, 2019		True	True
Windows SSH	7, 8, 8.1, 10 Server 2008 R2, 2012, 2012 R2, 2016, 2019 Windows SSH Other		True	True

Table 9: Supported platforms: Directories that can be searched

Platform	Version
Microsoft Active Directory	Windows 2008+ DFL/FFL
OpenLDAP	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.

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.

CAUTION: Facebook and Twitter functionality has been deprecated. Refer to the custom platform open source script provided on GitHub. Facebook and Twitter platforms will be remove in a future release.

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. Safeguard for Privileged Passwords 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). Safeguard for Privileged Passwords cannot check the validity or system impact of values entered for custom platforms.

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...`, then click **Next**.
7. On the **Choose Import Type** tab, select **Copy the virtual machine (create a new unique ID)**, then click **Next**.
8. On the **Choose Destination** tab, add the locations for the **Virtual machine configuration folder**, **Checkpoint store**, and **Smart Paging folder**, then click **Next**.
9. On the Choose Storage Folders tab, identify **Where do you want to store the imported virtual hard disks for this virtual machine?** then click **Next**.
10. Review the **Summary** tab, then click **Finish**.
11. In the **Settings**, **Add Hardware**, connect to Safeguard's MGMT and X0 network adapter.
12. 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 4. 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 4.

> 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. **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.

        You can update this information in **Administrative Tools** | **Settings** | **Appliance** | **Operating System Licensing**. For more information, see Operating system licensing on page 329.
   c. **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.

d. **Network (X0)**: For the X0 (public) interface, enter the IPv4 and/or IPv6 information, and **DNS Servers** information.

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 desktop client or use the web client

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

- (desktop client): Log in and download the desktop client. For more information, see Installing the desktop client on page 80.
- (web client): Use the web client. For more information, see Using the web client on page 72.

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 on page 465.

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, Safeguard for Privileged Passwords updates and networking changes can be made via the web management console by clicking **Setup**.

License: hardware, virtual, expiration

Safeguard for Privileged Passwords is made up of a core set of features, such as the UI and Web Services layers, and a number of modules.

Hardware appliance

The Safeguard for Privileged Passwords 3000 Appliance and 2000 Appliance ship with the following module which requires a valid license to enable functionality:

- Privileged Passwords

You must install a valid license for each Safeguard for Privileged Passwords module to operate. More specifically, if any module is installed, Safeguard for Privileged Passwords

will show a license state of **Licensed** and is operational. However, depending on which models are licensed, you will see 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 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.

Privileged sessions is available via a join to Safeguard for Privileged Sessions.

The virtual appliance will not function unless the operating system is properly licensed.

License expiration notice

As an Appliance Administrator:

- If you receive a "license expiring" notification, apply a new license using that module's **Update License** link:
  - (web client): Click the **Settings** menu on the left then click **Licensing** . Click + to upload a new license file.
  - (desktop client): Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Licensing**. Click + to upload a new license file.
- If all licensed modules have expired, you will be prompted to add a new license when logging in to the Safeguard for Privileged Passwords desktop client.
- If only one of the licensed modules have expired, apply a new module license by clicking + in **Administrative Tools** | **Settings** | **Appliance** | **Licensing**.

As a Safeguard for Privileged Passwords user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

For more information on adding or updating a Safeguard for Privileged Passwords license, see Licensing.

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

	Long Term Support (LTS) Release	Feature Release
Release frequency	**Frequency**: Typically, every 2 years **Scope**: Includes new features, resolved issues and security updates **Versioning**: The first digit identifies the LTS and the second digit is a 0 (for example, 6.0 LTS, 7.0 LTS, and so on).	**Frequency**: Typically, every 3 months **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 Release (for example, 6.6, 6.7, and so on).
Maintenance Release	**Frequency**:Typically, every 3 months during full support **Scope**: Includes critical resolved issues **Versioning**: A third digit designates the maintenance LTS Release (for example, 6.0.6 LTS).	**Frequency**:Only for highly critical issues **Scope**: Includes highly critical resolved issues **Versioning**: A third digit designates the maintenance Feature Release (for example, 6.6.1).
Support	Typically 3 years after the original publication date or until the next LTS is published (whichever date is later)	Typically 6 months after the original publication date or until the next feature or LTS Release is published (whichever date is later)

Release 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 Safeguard for Privileged Passwords (SPP) will work with the same LTS major version of Safeguard for Privileged Sessions (SPS). For the best experience, it is recommended you keep both their SPP and SPS in sync on the latest and supported version.

3

Using API and PowerShell tools

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

Using the API

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. Every function is exposed through the API to enable quick and easy integration regardless of what want to do or which language your applications are written. There are even a few things that can only only be done via the Safeguard SPP API. The Safeguard for Privileged Passwords API tutorial is available on GitHub at: https://github.com/oneidentity/safeguard-api-tutorial.

Access the SPP API

Safeguard for Privileged Passwords 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/notification/swagger/
```

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

  ```
  https://<Appliance IP>/a2a/notification/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 the former 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 Safeguard for Privileged Passwords Appliances. User accounts that you create in Safeguard for Privileged Passwords 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/v2/AuthenticationProviders`
     >
     > and parsing the returned JSON for the `RstsProviderScope` property.

     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/v2/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/v2/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 Safeguard for Privileged Passwords (**Settings | Safeguard Access | Login Control**) 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 11: 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 12: 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.
`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 13: 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

Operator	Example	Description/Notes
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

When using the `filter` parameter, you can use parenthesis () to group logical expressions. For example, `GET/Users?filter=(FirstName eq 'Jane' 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 '\''`

Safeguard PowerShell

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

Installation

The Safeguard for Privileged Passwords 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.

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) version 6.5 or higher
  - VMware Worksation 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 42.
- **Setup**: After the first setup, Safeguard for Privileged Passwords 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 on page 58.

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 or 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 on page 58.

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.

Migrating the VM

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

Virtual appliance backup and recovery

Use the following information to back up and recover a Safeguard for Privileged Passwords 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 hardware appliance cannot be restored on virtual appliances and backups taken from a virtual appliance cannot be restored on a hardware appliance.

Backup is handled via **Administrative Tools** | **Settings** | **Backup and Retention**. For more information, see Backup and Retention settings on page 343.

Recovery of the virtual appliance

A Safeguard for Privileged Passwords 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 on page 42.
2. Restore the backup. For more information, see Backup and Retention settings on page 343.

Cloud virtual appliance (for example, AWS or Azure

1. Redeploy using the deployment steps:
   - AWS: For more information, see Using AWS.
   - Azure: For more information, see Azure deployment on page 64.

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 on page 575.

It is recommended that terminal settings be 90 x 45 or larger. Smaller settings may result in a error like: `Screen dimension to small`. Also, the desktop client works the best at a resolution of 1024 x 768 or higher.

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

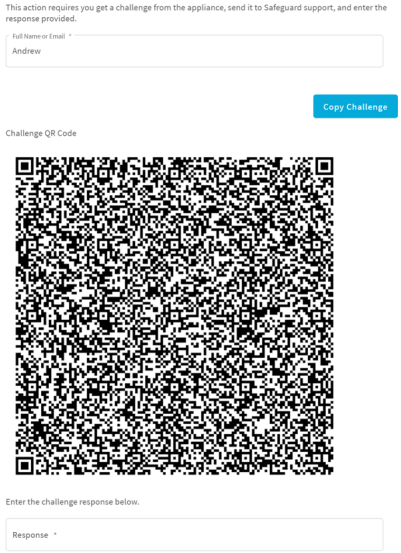
     This is read-only. You can re-run setup to change networking information.
   - **Power Options**
     You can reboot or shutdown the virtual appliance.
     a. Enter the reason you want to reboot or shutdown the virtual appliance.
     b. Click **Reboot** or **Shutdown**.
   - **Admin Password Reset**

     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. Do not refresh your screen.
        - Screenshot the QR code and send it to Support. Support will send back a challenge response that is good for 48 hours. Do not refresh your screen.

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



d. After the response is accepted, click **Reset Password**.

- **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.

- **Factory Reset** (hardware appliance)

  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. For more information, see Performing a factory reset on page 498.

  A virtual appliance is reset by the recovery steps to redeploy and not a factory reset. If you are attached to the console of a virtual machine, you will not have the Factory Reset option. The options are only available for hardware.

- **Lights Out Managment (BMC)** (hardware appliance)
  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.
  For more information, see Lights Out Management (BMC) on page 322.

5

Cloud deployment considerations

Safeguard for Privileged Passwords 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 on page 63.
- Azure Virtual Machine (VM): For more information, see Azure deployment on page 64.

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.

Restricting access to the web management kiosk for cloud deployments

The web management kiosk runs on port 9337 in AWS 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 and Azure). The Management web kiosk gives access to functions without authentication, such as pulling a support bundle or rebooting the appliance. In AWS, 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 Safeguard for Privileged Passwords.
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 Safeguard for Privileged Passwords.
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 TCP Rule
     Protocol: TCP
     Port Range: 655
     Source: Anywhere
     Description: Cluster VPN
   - 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**.

AWS deployment

Safeguard for Privileged Passwords (SPP) can be run in the cloud using Amazon Web Services (AWS).

To access the shared Amazon Machine Image (AMI) from AWS, contact your One Identity Salesperson and provide them your AWS Customer Name and Customer ID. The AMI will be shared with you and you will be provided the AMI ID. Refer to this AWS article for information on finding and using the shared AMI: Finding and Using Shared AMIs.

Disk size considerations

Safeguard for Privileged Passwords (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. 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 Safeguard for Privileged Passwords (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. Safeguard for Privileged Passwords hardware appliances have 32GB of RAM and 4 processors with at least 1TB of disk space.

View or change the cloud virtual appliance setup

You can view or change the virtual appliance setup.

You can use the Safeguard for Privileged Passwords 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 desktop client or API.

Azure deployment

Safeguard for Privileged Passwords (SPP) can be run in the cloud using Azure. A version of Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords 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) on page 549.

Disk size considerations

Safeguard for Privileged Passwords (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 Safeguard for Privileged Passwords (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

Safeguard for Privileged Passwords 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 465.

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 quarantine on page 575.

For more information, see Recovery Kiosk (Serial Kiosk).

To patch to a new version, use the desktop client or API.

Virtual appliance backup and recovery

Use the following information to back up and recover a Safeguard for Privileged Passwords 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 hardware appliance cannot be restored on virtual appliances and backups taken from a virtual appliance cannot be restored on a hardware appliance.

Backup is handled via **Administrative Tools** | **Settings** | **Backup and Retention**. For more information, see Backup and Retention settings on page 343.

Recovery of the virtual appliance

A Safeguard for Privileged Passwords 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 on page 42.
2. Restore the backup. For more information, see Backup and Retention settings on page 343.

Cloud virtual appliance (for example, AWS or Azure

1. Redeploy using the deployment steps:
    - AWS: For more information, see Using AWS.
    - Azure: For more information, see Azure deployment on page 64.

Setting up Safeguard for Privileged Passwords for the first time

Before 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 507.

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

Before Safeguard for Privileged Passwords 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 fails on page 540.

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 to your desktop client 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 451.

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

1. Make sure you have logged into the desktop client using the Authorizer Administrator account.
2. Customize the Password Rule. (Navigate to **Settings** | **Safeguard for Privileged Passwords Access** | **Password Rules**.)
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

   NOTE: A user can have more than one set of permissions. For a list of permissions granted to the different Safeguard for Privileged Passwords administrators, see Administrator permissions.

Step 3: Appliance Administrator configures the appliance

1. Log in to the desktop client using the Appliance Administrator account.
2. Navigate to **Settings** | **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 326.

3. Ensure the access request and password management features are enabled (**Settings** | **Access Request** | **Enable or Disable Services**). For more information, see Enable or Disable Services (Access and management services) on page 309.
4. (Optional) Enable or disable Application to Application (A2) and audit data sharing with Safeguard for Privileged Sessions (SPS) via **Settings** | **Appliance** | **Enable or Disable Services**. For more information, see Enable or Disable Services on page 319.
5. Configure the External Integration settings that apply (**Settings** | **External Integration**):

   a. Email: Configure the SMTP server to be used for email notifications. Safeguard for Privileged Passwords provides default email templates for most events, which can be customized.

   b. Identity and Authentication: Configure directory services such as Active Directory and LDAP servers to be used as identity and authentication providers for Safeguard for Privileged Passwords users. Configure Safeguard for Privileged Passwords 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.

   c. SNMP: Configure SNMP subscriptions for sending SNMP traps to your SNMP console when certain events occur.

   d. Starling: Join Safeguard for Privileged Passwords to Starling to take advantage of other Starling services, such as Starling Two-Factor Authentication.

   e. Syslog: Configure the syslog servers where event notifications are to be sent.

   f. Ticketing: Add external ticketing tracking system or track tickets not tied to an external ticketing system.

Step 4: User Administrator adds users

1. Log in to the desktop client 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 to the desktop client using the Asset Administrator account.
2. Add partitions and, optionally, delegate partition ownership to other users (Adding a partition).
3. (Optional) Set the following Profile settings (or edit the default rules and settings defined when the partition was added):
   a. Account Password Rules
   b. Change Password
   c. Check Password
   d. Password sync groups
4. (Optional) Create partition profiles or edit the default profiles created (Creating a profile).
5. Add assets to the appropriate partitions and profiles (Adding an asset).
6. 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 233.

Step 6: Security Policy Administrator adds access request policies

1. Log in to the desktop client using the Security Policy Administrator account.
2. Set Reasons. (**Settings** | **Access Request** | **Reasons**)
3. Configure Approval Anywhere. (**Settings** | **External Integration** | **Approval Anywhere**).
4. Add user groups (Adding a user group).
5. Add local or directory users to local user groups (Adding users to a user group).
6. Add account groups (Adding an account group).
7. Add accounts to account groups (Adding one or more accounts to an account group).
8. Add entitlements (Adding an entitlement).
9. Add users or user groups to entitlements (Adding users or user groups to an entitlement).
10. Create access request policies (Creating an access request policy).

Using the web client

The web client is functionally similar to the desktop client end-user view and useful for requestors, reviewers, and approvers. Many administration functions are available as well. The web client uses a responsive user interface design to adapt to the user's device, from desktops to tablets or mobile phones.

NOTE: In this documentation, you will see the following icons which denote the interface:

(web client)

(desktop client)

To change your photo in the web client, click the avatar **Change your photo** in the upper right. Select the image file, then click **Open**. You can right-click the photo to save or perform other photo options with the photo.

The pages available to you display on the left. You will see **Home** and, based on your role, you may also see **My Requests**, **Approvals**, **Reviews**, **Settings**, or a combination of those. You can customize the information you see on the pages. For more information, see Settings, version, and desktop Windows client (web client) on page 77.

You can reduce the left menu. In the upper left of the page, click to collapse or expand the menu.

Home

Click **Home** to go to the home page. The **Home** page is tailored to your user rights and permissions. If you are authorized by an entitlement to request, approve, or review access requests, then your **Home** page gives you a quick view to the access request tasks that need your immediate attention.

Based on your role, the dashboard displays **My Requests**, **Approvals**, and **Reviews**, the number of tasks in each queue, and the status of each task (for example, **Available**, **Denied**, **Revoked**, **Pending**) as well as whether the task is **Due Today**.

In addition to tasks based on your role, you can perform the following from the **Home** page:

- Customize the information that is displayed on each page. Click **Dashboard settings**. For more information, see Settings, version, and desktop Windows client (web client) on page 77.
- Read the **Message of the Day** from the Appliance Administrator. For more information, see Message of the Day on page 420.
- Create favorites for requests you make often. For more information, see Favorites (web client) on page 76.

Requester's Home page view

Click the **New Request** tile to open the **New Access Request** dialog, which lists the assets and accounts you are authorized to access. From this dialog you specify the assets, accounts and the type of access you are requesting, and additional details about the request.

For more information, see:

- Requesting a password release
- Requesting session access

Click **Requests** to view the requests awaiting action.

For more information, see:

- Taking action on a password release request
- Taking action on a session request

The **Favorites** pane (right pane) displays a list of requests you have marked as a favorite, providing a quick way to request access.

Favorites pane: Action bar buttons

Use the toolbar buttons at the top of the **Favorites** pane to manage your favorite requests:

- **New Favorite**: Select this button to create a new favorite request. Clicking this button displays the **New Access Request** dialog, allowing you to select the assets, accounts, type of access, and additional details about the request.
- Select this button to display additional options for managing your favorite requests:
  - Request Selected
  - Color Selected
  - Remove Selected

TIP: Select the check box to the left of a favorite request to use these additional buttons. Selecting the request itself will launch the **New Access Request** dialog, allowing you to edit and submit the request.

Submit a favorite request

To submit a favorite request, click the request or select the check box to the left of a request and select **Request Selected**. The **New Access Request** dialog displays allowing you to edit your selections or enter a required reason or comment before submitting it.

For more information, see:

- Desktop client favorite request

Approver's Home page view

Your job is to approve or deny the access requests listed on your **Home** page. Click **Approvals** to view the requests awaiting your approval. As an approver, unless you are also designated as a requester, you will see no favorites listed.

For more information, refer to these topics:

- Approving a password release request
- Approving a session request

Reviewer's Home page view

Your job is to review completed access requests listed on your Home page. Click **Reviews** to view the completed requests requiring your review. As a reviewer, unless you are also designated as a requester, you will see no favorites listed.

For more information, refer to these topics:

- Reviewing a completed password release request
- Reviewing a session request

My Requests (web client)

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

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 Request** page.
2. Follow the workflow steps. For more information, see Requesting a password release on page 121.

To create a favorite

You can create favorites for requests you make often. For more information, see Favorites (web client) on page 76.

To view and manage requests

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

- 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.
  - **All**: Requests in all states.
  - **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 Passwords 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 search-able elements. Or enter search characters. For more information, see Search box.

Approvals (web client)

If you are an approver, click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details: Select the request and the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click to approve all the selected requests. Optionally, enter a comment.

- Deny one or more request: Select the requests. Then, click to deny all the selected requests. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see.
- Search: For more information, see Search box on page 111.

For more information, see Approving a password release request on page 125.

Reviews (web client)

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

- View details: Select the request and the details display on the right of the page.
- Mark one or more request as reviewed: Select the requests. Then, click **Mark all the selected requests as reviewed**. A comment may be required or, if not required, added.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
- Search: For more information, see Search box on page 111.

Favorites (web client)

On your **Home** or **My Requests** page, you will see **My Favorites (number of favorites)**. You can quickly make requests by creating a favorite of requests you make often, then just click the favorite.

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 large icons or for small icons.

Add a favorite

1. To the right of **My Favorite Requests**, click **New Favorite**.
2. On the **Asset Selection** page, select the assets to access. Use the following approaches to quickly find the assets you want:
    - Click **Search** to search the **Asset**, **Network Address**, or **Platform**. For more information, see Search box on page 111.

- Once you've selected assets, the number of **Assets selected** displays in the lower left. You can toggle between **Show only selected** and **Show all**.
- In the lower right, select the number of **Items per page** that display. Click the arrows to move through the pages.

3. Click **Next**.
4. On the **Account & Access Type Selection** page, select the account for the asset. If there are several accounts associated with an asset:
   a. Click the **Select Account(s)** link.
   b. Select the account(s) for that asset.
   c. Click **OK**.
   d. Continue to select accounts for each asset.
5. Click **Next** to provide favorite details:
   a. Enter a **Name** for the favorite.
   b. Enter a **Brief Description**.
   c. Select the color of the favorite's tile.
6. Click **Add**.

Use and manage a favorite

Once a favorite has been created, you can use and make changes to the favorite.

1. Click the ⋮ menu on the right of the favorite and perform a task:
   - Click **Submit Request** to submit the request and launch the request workflow. Follow the workflow steps. For more information, see Requesting a password release on page 121.
   - Click **Change Color** to change the color of the favorite. This is useful to color code types of requests.
   - Click **Remove** to delete the favorite.

Settings, version, and desktop Windows client (web client)

You can control page displays, check the version, or download the Safeguard for Privileged Passwords Windows client.

1. In the upper right corner, next to your user name, click ▼ then **Application Settings** to proceed. Or, from the **Home** page, click **Dashboard settings**.
2. Select any of the following tabs, which are available based on your role and permissions.

- **General** tab:
  - **Pages**: Toggle the pages which are available on or off. If your role changes, you can change the display in the future.
  - **Homepage**: Select the page you want to see first when you log on.
  - **About**: The **Appliance Version** displays.
  - **Download Windows Client**: Click to download the Windows desktop client.
- **Home** tab, **Home Page Widgets** :
  - **Message of the Day** and **My Request Favorites**: Toggle selections or off.
  - **Tile Set** (Approvals, Reviews, and so on): Toggle selections or off. Then, select the statuses you want to display. For example, to view your available requests, you would set the **Tile Set: My Requests** on then select the **Available** check box. What you can set is based on your role and permissions.
- **Approvals** tab (if available): On the **Approvals Widgets** page, control available widgets, if any.
- **Requests** tab (if available): On the **My Request Widgets** page, toggle what you want to display on on or off.
- **Reviews** tab (if available): On the **Review Widgets** page, control available widgets, if any.

Change password (web client)

You can change your password.

To change the password

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

FIDO2 keys (web client)

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 **Manage FIDO2 Keys**. The name and date each existing key was registered and last used displays.
3. 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.

Log out (web client)

Always securely log out of the web client.

To log out

1. In the upper right corner, next to your user name, click .
2. Click **Log out** to securely exit the Safeguard for Privileged Passwords web client.

8

Getting started with the desktop client

To define and enforce security policy for your enterprise, you must first install the desktop client application which gives you access to the **Administrative Tools**.

These topics explain how to install, start, and uninstall the Safeguard for Privileged Passwords desktop client application:

Installing the desktop client

Starting the desktop client

Uninstalling the desktop client

Installing the desktop client

During initial installation and when applying a patch, make sure the desktop client file is the one supplied with the appliance version. If the versions are not compatible, errors will occur.

NOTE: PuTTY is used to launch the SSH client for SSH session requests and is included in the install. The desktop client looks for any user-installed PuTTY in the following locations:

- Any reference to putty in the PATH environment variable
- `c:/Program Files/Putty`
- `c:/Program Files(x86)/Putty`
- `c:/Putty`

If PuTTY is not found, the desktop client uses the version of PuTTY that it installed at:

`<user-home-dir>/AppData/Local/Safeguard/putty`.

If the user later installs PuTTY in any of the locations above, the desktop client uses that version which ensures the user has the latest version of PuTTY.

Installing the Safeguard for Privileged Passwords desktop client application

1. To download the Safeguard for Privileged Passwords desktop client Windows installer .msi file, open a browser and navigate to:

   https://<Appliance IP>/Safeguard.msi

   Save the **Safeguard.msi** file in a location of your choice.
2. Run the MSI package.
3. Select **Next** in the **Welcome** dialog.
4. Accept the **End-User License Agreement** and select **Next**.
5. Select **Install** to begin the installation.
6. Select **Finish** to exit the desktop client setup wizard.
7. Check your desktop resolution. The desktop client works the best at a resolution of 1024 x 768 or greater.

Installing the Desktop Player

CAUTION: If the Desktop Player is not installed and a user tries to play back a session from the Activity Center, a message like the following will display: `No Desktop Player. The Safeguard Desktop Player is not installed. Would you like to install it now?` **The user will need to click Yes to go to the download page to install the player following step 2 below.**

1. Once the Safeguard for Privileged Passwords installation is complete, go to the Windows **Start** menu, **Safeguard** folder, and click **Download Safeguard Player** to be taken to the One Identity Safeguard for Privileged Sessions - Download Software web page.
2. Follow the *Install Safeguard Desktop Player* section of the player user guide found here:
   a. Go to One Identity Safeguard for Privileged Sessions - Technical Documentation.
   b. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.
3. For Safeguard Desktop player version 1.8.6 and later, ensure your signed web certificate has a Subject Alternative Name (SAN) that includes each IP address of each of your cluster members. If the settings are not correct, the Safeguard Desktop Player will generate a certificate warning like the following when replaying sessions: `Unable to verify SSL certificate. To resolve this issue, import the appropriate certificates including the root CA.`

New Desktop Player versions

When you have installed a version of the Safeguard Desktop Player application, you will need to uninstall the previous version to upgrade to a newer player version.

Starting the desktop client

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

To start the desktop client application

1. From the Windows Start menu, choose **Safeguard**.
2. On the server selection screen, enter or select the server's network DNS name or IP address to connect to the appliance over the network and click **Connect**.

   NOTE: When entering an IPv6 address, enclose the IPv6 address in square brackets.
3. You will see a message like: `You'll now be redirected to your web browser to complete the login process.` You can select: `Don't show this message again.` Then, click **OK**.
4. On the user login screen, enter your credentials and click **Log in**.
   - User Name: Enter your user or display name. Do not include spaces in the User Name.

     NOTE: When using directory account credentials, you have the option to enter your domain\name.
   - Password: Enter the password associated with the user entered above.
5. If your Safeguard for Privileged Passwords user account requires you to log in with secondary authentication, enter the secure password token code, or other authentication for your authentication service provider account and click **Submit**.

   NOTE:The type and configuration of the secondary authentication provider (for example, RSA SecureID, FIDO2, One Identity Starling Two-Factor Authentication, 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 Safeguard for Privileged Passwords with secondary authentication.
6. When login is successful, you can close the web browser and return to the Safeguard application.

To remove server DSN names or IP addresses no longer used

The DSN name or IP address on the server selection screen may be no longer used. If you want to remove one or more selections, you can edit the `user.config` file using a text editor like Notepad.

1. Go to:

   ```
   C:\Users\<YourSafeguardUserName>\AppData\Local\One_Identity_
   LLC\Client.Desktop.UI.exe_Url_<UniqueGUID\<ClientVersion>\user.config
   ```
2. Make a backup copy of `user.config` in case you want to return to the file.
3. Open the file and edit the following section to list only the addresses you want:

```
<setting name="ClusterHistory" serializeAs="Xml">
<value>
<ArrayOfString xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<string>10.5.33.57</string>
</ArrayOfString>
</value>
</setting>
```

4. Save the updated file.
5. Log on to verify the correct selections display.

Uninstalling the desktop client

You can uninstall a desktop client.

To uninstall the desktop client

1. In the Windows Control Panel, open **Programs and Features**.
2. Right-click the Safeguard for Privileged Passwords application and choose **Uninstall**.

9

Using the desktop client

Safeguard for Privileged Passwords has two graphical user interfaces that allow you to manage password and session requests, approvals, and reviews for your managed accounts and systems:

- Windows desktop client: The desktop client consists of an end-user view and an administrator view. The administrative functionality is dynamically enabled based on the user's permissions. The desktop client user interface information follows.
- Web client: The web client is functionally similar to the desktop client end-user view. For more information, see Using the web client on page 72.

NOTE: In this documentation, you will see the following icons which denote the interface:

(web client)

(desktop client)

Desktop client toolbar

The toolbar along the top-right corner of the Safeguard for Privileged Passwords console, has these controls:

- User avatar: Modify personal information, view notifications, or log out of the Safeguard client. For more information, see User information and log out (desktop client) on page 86.
- Settings: Configure the desktop client application, including notifications and **Home** page widgets, or view product information, including contact information. For more information, see Settings (desktop client) on page 84.

Settings (desktop client)

The desktop client console **Settings** ( ) allows you to configure the desktop client application.

Notifications

Use the following options to control notifications within Safeguard for Privileged Passwords:

- **Run in the System Tray** when you close the application.

  When you enable the **Run in the System Tray** option, you cannot modify the toast notifications option. However, when you disable the **Run in the System Tray** option, you can enable or disable toast notifications.

  > NOTE: When you enable the **Run in the System Tray** option, you cannot modify the toast notifications option because in that mode, you always get notifications.

- **Enable Toast Notifications** to display event alerts on your console.

  Toast notifications are alerts that appear when the desktop client application is not the active foreground application: for example, when you are in another application or when you have minimized the desktop client.

Reset Notifications: Click **Reset Notifications** to reenable any notifications pop ups that have been preciously suppressed.

Widgets

Click the toggles to enable (toggle on) or disable (toggle off) the **Home** page widgets:

- Requests
- Approvals
- Reviews

All widgets are enabled by default, indicating that the corresponding controls display on your **Home** page. The toggles appear blue with the switch to the right when a widget is enabled, and gray with the switch to the left when a widget is disabled.

About dialog tab

Click **About Safeguard for Privileged Passwords** to display the following information.

- **About**: The trademark and copyright information
- **Contact**: Information about how to get in touch with One Identity
- **Components**: A list of third-party components used in Safeguard for Privileged Passwords
- **Third Party License Text**: The license text for third-party components that require this text to be included in the product documentation

User information and log out (desktop client)

On the desktop client, click the user avatar (or the Welcome link with your user name) to modify your personal information, manage email notifications, view current notifications, or log out of Safeguard for Privileged Passwords.

My Account

Click **My Account** to modify your personal information and manage your email notifications.

> NOTE: Safeguard for Privileged Passwords Active Directory users cannot use **My Account** to modify their email address, phone number, or change their password. They must do these actions in Active Directory

To update your personal information

1. From the toolbar, select your user avatar and choose **My Account**. Perform any of the following:
   - To change your image, select **Change Photo**.
   - To change your email address or **Contact Information**, type into the appropriate box.
2. Click **Done** to close the My Accounts pane.

To change your user password

1. From the toolbar, select your user avatar and choose **My Account**.
2. To change your user password, click **Change Password** and complete the information.
3. Click **Done** to close the My Accounts pane.

To manage your FIDO2 keys

At least one 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. From the toolbar, select your user avatar and choose **My Account**.
2. Click **Manage FIDO2 Keys**. The name and date each key was registered and last used displays.
   - Click **Edit** to change the name then click **Save**. Click **Cancel** to leave the editing operation.

- Click **Delete** to delete a key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.
- Click **Register New FIDO2 Key** to add a 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.

3. Click **Done** to close the My Accounts pane.

For more information, see Requiring secondary authentication log in.

To manage the notifications you receive

1. From the toolbar, select your user avatar and choose **My Account**.
2. Click **Manage Email Notifications**.

   The **Manage Email Notifications** dialog displays the type of events for which you are receiving email notifications.

   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.

3. From this dialog, you can define the types of events for which you want to receive notifications.

   By default, all events are selected. Clear the check box for any events for which you do not want to receive an email notification.

   TIP: Select the check box next to the **Events** heading to select all of the events in the list. Similarly, clear the check box next to the **Events** heading to clear all of the event check boxes.

4. Click **OK** to save your selections and close the dialog.
5. Click **Done** to close the **My Accounts** pane.

Log Out

Click **Log Out** to log out of the Safeguard for Privileged Passwords desktop client.

Desktop client favorite request

If you are designated as a requester, the desktop client allows you to add an access request as a **Favorite** to your **Home** page. **Favorites** are unique for the user; they are available when you log in to the desktop client or the web client.

You can create a favorite request from your **Favorites** pane on your **Home** page or from the **New Access Request** dialog when creating or editing an access request.

To create a favorite request from your Home page

1. In the **Favorites** pane, click **+ New Favorite**.
2. In the **New Access Request** dialog, specify the assets, accounts, and type of asset to be included in the access request.
   a. On the **Asset Selection** tab, select the assets to be included in the access request.
   b. On the **Account & Access Type** tab, select the accounts to be included in the access request and the type of access being requested for each selected account. The accounts include linked accounts, if any. For more information, see Linked Accounts tab (user) on page 448.
      - **Account**: The available account appears in the **Account** column. When an asset has multiple accounts available, click **Select Account(s)** to select an account from the displayed list.
      - **Access Type**: The type of access request appears in the **Access Type** column. When multiple access request types are available, this value appears as a hyperlink. Click this hyperlink to select the access type.
3. Click the **Add to Favorites** button.
4. In the **Add to Favorites** dialog, specify the following:
   a. **Name**: Enter a name for the request.
   b. **Description**: Enter descriptive text about the request.
   c. **Color**: Select the icon color to be used to display the request in your **Favorites** pane.

   Click **Add**.

   The dialogs closes and the new favorite are added to the **Favorites** pane on your **Home** page.

To create a favorite request from the New Access Request dialog

1. At the bottom of the **New Access Request** dialog, click the **Add to Favorites** button when you are creating a new request. The **Add to Favorites** button is enabled when you select the minimum required information (that is, at least one asset, account, and an access type) for the access request.
2. In the **Add to Favorites** dialog, specify the following:

a. **Name**: Enter a name for the request.

b. **Description**: Enter descriptive text about the request.

c. **Color**: Select the icon color to be used to display the request in your Favorites list.

3. Click **Add**.

To change a favorite request's icon color

1. At the top of the **Favorites** pane, click the button to display the **Color Selected** button.
2. Select the check box to the left of the favorite request to be changed. Selecting a favorite request, instead of the check box, displays the **New Access Request** dialog to edit and submit the access request.
3. Click **Color Selected**.
4. In the **Settings** dialog, choose a color and select **OK**.

   The icon for the favorite now appears in the color you selected.

To remove a favorite request

1. At the top of the **Favorites** pane, click the button to display the **Remove Selected** button.
2. Select the check box to the left of the favorite request to be removed. Selecting a favorite request, instead of the check box, displays the **New Access Request** dialog to edit and submit the access request.
3. Click the **Remove Selected** button.
4. Select **Yes** to confirm.

Desktop client navigation pane

In the desktop client, the **Home** page left navigation pane has these links.

- Home: Where you view and take action on the access request tasks that need your immediate attention. As a requester, it also provides access to your list of **Favorite** access request queries.
- Dashboard: Where Security Policy Administrators can audit access requests. Where Asset Administrators can view information regarding accounts that are failing different types of tasks.
- Activity Center: Where you can search for and review activity for a specific time frame.
- Reports: Where you can view and export entitlement reports that show you which assets and accounts a selected user is authorized to access.

- Administrative Tools: Where you add all the objects you need to write access request policies, such as users, accounts, and assets. Where you define and management all of the administrative Safeguard for Privileged Passwords settings.

Home

Click **Home** to go to the home page. The **Home** page is tailored to your user rights and permissions. If you are authorized by an entitlement to request, approve, or review access requests, then your **Home** page gives you a quick view to the access request tasks that need your immediate attention.

Based on your role, the dashboard displays **My Requests**, **Approvals**, and **Reviews**, the number of tasks in each queue, and the status of each task (for example, **Available**, **Denied**, **Revoked**, **Pending**) as well as whether the task is **Due Today**.

In addition to tasks based on your role, you can perform the following from the **Home** page:

- Customize the information that is displayed on each page. Click **Dashboard settings**. For more information, see Settings, version, and desktop Windows client (web client) on page 77.
- Read the **Message of the Day** from the Appliance Administrator. For more information, see Message of the Day on page 420.
- Create favorites for requests you make often. For more information, see Favorites (web client) on page 76.

Requester's Home page view

Click the **New Request** tile to open the **New Access Request** dialog, which lists the assets and accounts you are authorized to access. From this dialog you specify the assets, accounts and the type of access you are requesting, and additional details about the request.

For more information, see:

- Requesting a password release
- Requesting session access

Click **Requests** to view the requests awaiting action.

For more information, see:

- Taking action on a password release request
- Taking action on a session request

The **Favorites** pane (right pane) displays a list of requests you have marked as a favorite, providing a quick way to request access.

Favorites pane: Action bar buttons

Use the toolbar buttons at the top of the **Favorites** pane to manage your favorite requests:

- **New Favorite**: Select this button to create a new favorite request. Clicking this button displays the **New Access Request** dialog, allowing you to select the assets, accounts, type of access, and additional details about the request.
- Select this button to display additional options for managing your favorite requests:
  - Request Selected
  - Color Selected
  - Remove Selected

TIP: Select the check box to the left of a favorite request to use these additional buttons. Selecting the request itself will launch the **New Access Request** dialog, allowing you to edit and submit the request.

Submit a favorite request

To submit a favorite request, click the request or select the check box to the left of a request and select **Request Selected**. The **New Access Request** dialog displays allowing you to edit your selections or enter a required reason or comment before submitting it.

For more information, see:

- Desktop client favorite request

Approver's Home page view

Your job is to approve or deny the access requests listed on your **Home** page. Click **Approvals** to view the requests awaiting your approval. As an approver, unless you are also designated as a requester, you will see no favorites listed.

For more information, refer to these topics:

- Approving a password release request
- Approving a session request

Reviewer's Home page view

Your job is to review completed access requests listed on your Home page. Click **Reviews** to view the completed requests requiring your review. As a reviewer, unless you are also designated as a requester, you will see no favorites listed.

For more information, refer to these topics:

- Reviewing a completed password release request
- Reviewing a session request

Dashboard

The **Dashboard** contains operational information that allows administrators with the proper permissions to view and manage access requests and accounts failing tasks from a single location.

- Access Requests: Displays information about access requests in different stages of the workflow.
- Account Automation: Displays information about accounts that are failing different types of tasks.

Access Requests

The **Access Requests** tab on the Dashboard allows Security Policy Administrators to review and manage access requests from a single location. Clicking one of the access request tiles across the top of the view displays additional information about the access requests belonging to that category. In addition, you can review the request workflow, launch a live session, terminate a session, or revoke a specific request.

This dashboard is available to Safeguard for Privileged Passwords users assigned the following administrative permissions:

- Auditor: Read-only view.
- Security Policy: Full control.

Access requests: Tiles

- **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.
- **Pending Approval**: Displays a list of access requests to be approved.
- **Pending Review**: Displays a list of access requests to be reviewed.
- **Open Requests**: Displays a list of all currently opened access requests, including session requests and password release requests.

Access requests: Toolbars

Use the toolbar at the top of the details grid to perform the following tasks.

- **Workflow**: 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.
- **View Live Session**: Select to view a live session for the selected session request. Clicking this button launches the Desktop Player allowing you to follow an active session.

  If the Desktop Player is not installed, see Installing the desktop client, **Installing the Desktop Player** section.

  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 Session**: Select to terminate the live session for the selected session request.
- **Revoke 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.

  You can convert timestamps to local time, if necessary. For more information, see Converting time stamps on page 106.
- **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.

Viewing details

Additional detailed information is available for access requests listed in the request grids on the **Access Requests** view.

To see the details of an access request

1. Double-click a request to view additional details.
2. Double-click to close the request details.

   NOTE: Clicking **Refresh** at the top of the view also closes the details in addition to retrieving the latest access requests.

Account Automation

The **Account Automation** tab on the **Dashboard** allows Asset Administrators to view information regarding accounts that are failing different types of tasks. This dashboard includes both automated and manual tasks in the failure results. Clicking one of the failure

task tiles across the top of the view displays additional information about the accounts belonging to that category.

This dashboard is available to Safeguard for Privileged Passwords users assigned the following administrative permissions:

- Asset Administrator: Full control for accounts related to all Safeguard for Privileged Passwords assets
- Auditor: Read-only view
- Delegated Partition Owner: Control for accounts related to the accounts and assets managed through delegation

Account Automation: Tiles

- **Password Check Failures**: Displays a list of accounts where password check tasks failed.
- **Password Change Failures**: Displays a list of accounts where password change tasks failed.
- **SSH Key Change Failures**: Displays a list of accounts where SSH key change tasks failed.
- **Suspend Account Failures**: Displays a list of accounts where suspend tasks failed.
- **Restore Account Failures**: Displays a list of accounts where restore tasks failed.

Account Automation: Toolbar

Use the toolbar at the top of the details grid to perform the following tasks.

- **Rerun task**: Select to rerun 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.
- You can convert timestamps to local time, if necessary. For more information, see Converting time stamps on page 106.
- **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.

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 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 507.

Activity Center: Main page toolbar

The toolbar at the top of the main **Activity Center** page contains these options.

- **Clear**: Resets the current search criteria back to the default settings (all activity occurring within the last 24 hours.)
- **Schedule**: Allows you to define when the activity audit log report is to be generated and sent via email as well as the format of the report (.csv or .json). For more information, see Scheduling an activity audit log report on page 99.
- **Open**: Allows you to access previously saved search and scheduled reports.
- **Save**: Saves the current search criteria which can be used later to generate the report. For more information, see Saving search criteria on page 97.
- **Run** button: Generates an activity audit log report based on the search criteria specified.

In addition, query tiles display the criteria you have applied to search the activity data. By default, only the **Activity category** and **Time frame** tiles display. Use the **+ Add** button to specify additional query criteria to retrieve the information you are looking for. For more information, see Applying search criteria on page 95.

Activity Center: Results page toolbar

Once an activity audit log report is generated, the results page contains the search results grid and these toolbar options.

- **Back**: Takes you back to the query page where you can modify the search criteria.
- **Refresh**: Closes the details and updates the search results page.

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 tiles provided you can specify search criteria to retrieve specific information from the activity audit log. The search criteria available includes:

- Activity category (to narrow parameters and event details)
- Time frame
- User

- Asset
- Account
- Search keyword or value: For sessions, you can search by keyword or value.

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. From the Safeguard for Privileged Passwords desktop Home page, select **Activity Center**.
2. **I would like to see** defaults to **All Activity**. Click the tile to limit the report to a particular type of activity and select the activity category to be included in the report.
3. **Occurring within the** defaults to **Last 24 Hours**. To specify a different time frame, click the tile and select the time frame to be included in the report. If using the **Custom** option, specify the custom date and time range.
4. Click the **+Add** button to further filter results. The options to add are based on the selections you made and may include user, asset, or account. When you add filters, additional tiles display such as: **involving the asset**.
   - If you select **Add User**, you can specify one user. A tile with the user displays.
   - If you select **Add Asset**, you can select an asset. A new tile with the asset displays. When an account is specified, the **Add Asset** option is not available.
   - If you select select **Add Account**, you can select the account. When an asset is specified, the **Add Account** option is not available.
5. To search session activity for a specific keyword or value.
   a. Change the activity category (**I would like to see**) to **Session Specific Activity (or In-Session Activity)**.
   b. Click the **+ Add** button and select **Add Search value**.
   c. In the **Enter a Search Value** dialog, enter the keyword or value (e.g., regedit) and click **OK**.

   An additional tile appears listing the keyword or value specified. If you later change the activity category, the keyword tile will be dimmed indicating it will not be included in the query.
6. To remove or edit your selections, use the icons in the upper-right corner of a query tile:
   - **Clear**: Resets the value back to the default. **Clear** is only available for Activity category and Time frame.
   - **Delete**: Removes search criteria tiles you added.
   - **Edit**: Displays the corresponding dialog allowing you to modify your selection. You can also click a query tile to edit your selection.

Saving 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. From the Safeguard for Privileged Passwords desktop Home page, select **Activity Center**.
2. Specify the search criteria to be used to generate the desired report. For more information, see Applying search criteria on page 95.
3. Click **Save**.
4. In the **Save Search** dialog, enter the following information:
   a. **Name**: Enter a name for the search.
   b. **Description**: Optionally, enter descriptive text to describe the search.
5. Click **OK**.
6. To run a previously saved search, click **Open**.
   a. Select a search from the list. (The criteria for the selected search is displayed in the right pane.)
   b. Click **Open**.

   The query tiles for the selected search appear in the Activity Center page, where you can then select **Run** to generate the report.

Generating an activity audit log report

To generate an activity audit log report

1. From the Safeguard for Privileged Passwords desktop Home page, select **Activity Center**.
2. Use the query tiles 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 95.
3. Click **Run**.

   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 window.)

   For example, the "All Activity" report displays the following information for each event.

   - State: The left-most column displays one of the following regarding the availability of a recorded session:

- Blank: Indicates that there is no recorded session available.
- (green dot): Indicates that a live session is taking place. A Security Policy Administrator can click this button to launch the Desktop Player to follow what is happening in the current session.
- **Play**: Indicates that there is a recorded session available locally on the appliance. Clicking this button launches the Desktop Player to play back the selected recording.
- **Download**: Indicates that there is a recorded session available on the archive server. Clicking this button downloads the recording for play back.

NOTE: These icons only appear on an "All Activity" or "Session Specific Activity" report.

- **User**: The name of the user who triggered the event.
- **Date**: The date and time the event occurred.
- **Activity Category**: The category that defines the type of activity that occurred.
- **Event**: The event that occurred. Double-click an event to view or hide event details.

Actions once a report is generated

Once a report is generated, you can use the buttons above the grid as described below.

- **Time frames**: To rerun the report using a different time frame, select one of the following links, specify the time range, then click **Run**.
  - Last 24 Hours (default)
  - Last 7 Days
  - Last 30 Days
  - Last 60 Days
  - Last 90 Days
  - Custom
- **Workflow**: 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. For more information, see Replaying a session on page 142.
- **Run**: Select to generate the report using the specified time frame.
- **Export**: Right-click to select **Export as CSV** or **Export as 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. Once the report is exported, you can convert

timestamps to local time, if necessary. For more information, see Converting time stamps on page 106.

- **Schedule**: Select to schedule the generation of the activity audit log report. For more information, see Scheduling an activity audit log report on page 99.
- **Save**: Select to save the current search criteria to reuse the search later. For more information, see Saving search criteria on page 97.
- **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

Safeguard for Privileged Passwords 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. From the Safeguard for Privileged Passwords desktop Home page, select **Activity Center**.
2. Specify the search criteria to be used to generate the desired report. For more information, see Applying search criteria on page 95.
3. Click **Schedule**.
4. If the **Configure Email** dialog displays, click **Configure Email** to add your email in the **My Account** dialog. (The email server must be configured in Safeguard for emails to be sent.)
5. In the **Schedule Report** dialog, enter the following information:
   a. **Name**: Enter a name for the report.
   b. **Description**: Optionally, enter descriptive text for the report.
   c. **Send To**: Read-only field displaying the email address of the user currently logged into the Safeguard for Privileged Passwords client. This field is required. If this field is blank, you must set your email address in **My Account**. For more information, see User information and log out (desktop client) on page 86.
   d. 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.
   e. To set the schedule, select **Run Every** to run the job 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.

  - **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 **-** delete 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 AM**
  - **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 that 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 20:00:00 PM** and **Repeat 2**.

- **Time Zone**: Select the time zone.

6. Click **Schedule Report**.

Editing or deleting a saved search or scheduled report

Click the **Open** toolbar button to display a list of saved searches and scheduled reports. From this dialog, you can delete or edit a saved search or scheduled report.

1. From the Safeguard for Privileged Passwords desktop Home page, select **Activity Center**.
2. From the Activity Center dialog, click **Open**.

   The **Select a Saved Search** dialog displays, which contains a list of all saved searches and scheduled reports including the **Name**, **Description**, **Schedule**, and saved **Format** (.csv or .json).
3. Select a saved search or scheduled report from the list.

   The search criteria defined for the search or report appear in the right pane.
4. Click one of the toolbar buttons or right-click commands.
   - **Delete**
   - **Edit**
   - **Edit Schedule**
5. If you selected **Delete**, click **Yes** in the confirmation dialog.

   The selected search or schedule will be removed from the list.
6. Depending on the type of search selected (saved search or scheduled report), the following editing capabilities are available:
   - **Edit** displays the **Save Search** dialog, allowing you to modify the name and description for a saved search or schedule. The **Edit** button is available for a saved search or a scheduled reports with an interval of **Never**.
   - **Edit Schedule** displays the **Schedule Report** dialog, allowing you to modify the schedule settings for a scheduled report. The **Edit Schedule** button is available for a saved search or a scheduled report. Using the command for a saved search allows you to convert it to a scheduled report.

NOTE: Clicking the **Open** button at the bottom of the **Select a Saved Search** dialog closes the dialog and returns you to the Activity Center view, where the query tiles for the selected search or report appear. You can then select **Run** to generate the report.

Viewing event details

Additional detailed information is available for some activity events.

To see the details of a specific event

1. Double-click an event to view additional details.
2. On Password management events, select **Details** to see the details of the password change or check tasks.
3. Double-click to close the event details.

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 tiles to specify the content of the report, and click **Run**.

   TIP: You can change the activity category tile to specify that you want to see **Access Request Activity**, **Session Specific Activity** events, or both.

2. 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.

   TIP: If you ran an all activity report, use the filter in the Events column to locate the access request activities.

3. For session requests that have **Record Session** enabled in the policy, you can play back a recorded or active session:

   a. Locate an access request session event and click **Play** to launch the Safeguard for Privileged Passwords Desktop Player. The following activities may be available to you:

      - A (green dot) indicates the session is "live". A user with Security Policy Administrator permissions can click this icon to follow an active session.
      - If the session recording has been archived and removed from the local Safeguard for Privileged Passwords file system, you will see a **Download** button instead of a **Play** button. Click **Download** to download the recording and then click **Play**.

   b. Accept the certificate to continue.

c. Use one of the following methods to play back the session recording:
    - Click ▶**Play Channel** from the toolbar at the top of the player.
    - Click the thumbnail in the upper right corner of the Information page.
    - Click ▶**Play Channel** next to a channel in the Channels pane.

4. For SSH session requests that have the **Enable Command Detection** option selected in the policy, you can review a list of the commands and programs run during the session.

   For RDP session requests that have the **Enable Windows Title Detection** option selected in the policy, you can review a list of all the windows opened on the desktop during the privileged session.

   a. Click the **Sessions Events** link above the transaction grid to view a list of all the session events and recordings available for the selected session.

   b. To see the individual events that occurred during a particular Initialize Session transaction:
      - Click **Show Details** to display additional information about the Initialize Session event, including Session Events.
      - Click the **events** link to view the commands and programs run during that particular Initialize Session event

   The **Session Events** dialog displays listing the events with a time stamp showing when the event occurred as well as in which recording if multiple recordings were created.

Filtering report results

To find information in an activity audit log report or entitlement report, use the controls in the grid heading row to filter the data. When a column has selected filter criteria, Safeguard for Privileged Passwords highlights the ▼ filter symbol.

To filter columns

1. Click ▼ **Filter** to open the filter list.
2. Select individual objects in the filter list to display specific information.

   NOTE: You can also choose the **Select All** check box at the top of the filter list and clear individual objects.

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.
3. To specify a secondary sort order, press the SHIFT key and then click the heading of the column to be used for the secondary sort order.

To move columns

To change the order of the columns, click the heading of the column to be moved. Drag and drop the column to a new location within the grid.

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.

Reports

Reports allows the Auditor and Security Policy Administrators to view and export entitlement reports that show which assets and accounts a selected user is authorized to access. Reports may be exported in .csv or .json format.

Reports toolbar

The toolbar at the top of **Reports** contains these options.

- **Refresh**: Updates the entitlement report.
- **Export**: Used to create a .csv or a .json file of the report. 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.

Once the report is exported, you can convert timestamps to local time, if necessary. For more information, see Converting time stamps on page 106.

Entitlement reports

Safeguard for Privileged Passwords provides these entitlement reports.

- **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.

Running an entitlement report

You can run an entitlement report.

To run an entitlement report

1. From the Safeguard for Privileged Passwords desktop Home page, select **Reports**.
2. In the first drop-down, choose a type of report: **User**, **Asset**, or **Account**.
3. In the second drop-down, you can select **All** or you can select **Browse** to select one or more objects for the report. If you select multiple objects, the selected objects display in the center of the page. Click a selected object to display the object's information at the bottom of the page.
4. The top of the report displays the following information.

   User:

   - **Name**: The name of the user.
   - **Username**: The user name used for authentication.
   - **Domain name**: The name of the domain of the user.
   - **Accounts**: Number of accounts each user is allowed to access.
     If an access request policy allows password access to linked accounts, an account may display twice: once based on the policy scope and a second time because it is a linked account. In the bottom grid, see the **From Linked Account** column. For more information, see Access Config tab on page 284.

   Asset:

   - **Name**: The name of the asset.
   - **Accounts**: Number of accounts on this asset that can be accessed.
   - **Requesters**: Number of users allowed to request access to the asset's accounts.
   - **Partition**: The name of the partition to which the asset belongs.
   - **Users**: The name of the requesters allowed to request access.

   Account:

   - **Name**: Name of the account.
   - **Asset**: Name of the asset associated with the account.
   - **Domain Name**: If applicable, the domain of the account.
   - **Requesters**: Number of requesters allowed to access an account.
5. Select an item from the top pane to view additional detail in the lower pane.
   For entitlements by assets, you can continue to drill down into the details of an item.

For example, you can view both the **Total Accounts** tab and the **People** tab to see more details about the users that can request the accounts on an asset. Select an item from the results to drill down further into the details about the users and the accounts.

6. To filter the results, use the filter control in the column heading. For more information, see Filtering report results on page 103.

To export the report

1. To export, select **Export** and then select **Export as CSV** or **Export as JSON**. Save the file to the location desired. 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.
2. Once the report is exported, you can convert time stamps to local time, if necessary. For more information, see Converting time stamps on page 106.

To run the report

Click the **Run** button to generate the report.

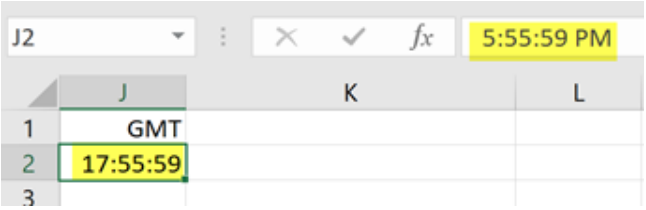
Converting time stamps

When you export .csv or .json files, the time stamp will be in UTC/GMT time. You can convert the time to your local time.

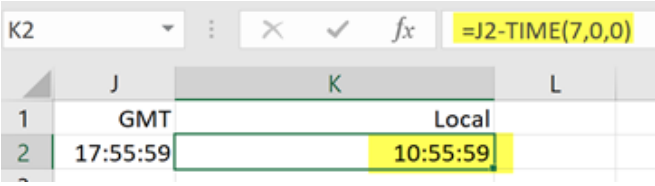
.csv opened in Excel

1. Identify how many hours different your local time is from the UTC or GMT exported by googling "UTC to my time." The value will be within the -12 to 12 range.
2. In the column to the right of the time stamp, enter one of the following formulas. These examples assume the exported time is in cell J1 and the exported time is -7 hours after the current local time.
   - =J1-TIME(7,0,0)
   - =J1+(-7 / 24)

   Below, the exported time stamp is 17:55:59 GMT (5:55:59 p.m.).



The formula converts the time to the local time stamp of 10:55:59 p.m.



.json

You can find code to convert JSON UTC time to local time. One possible source:

https://stackoverflow.com/questions/42376914/json-utc-time-to-local-time

Administrative Tools

The **Administrative Tools** allow you to add all the objects you need to write access request policies, such as users, accounts, and assets. From this view, you can also configure all of the Safeguard for Privileged Passwords settings.

NOTE: You must have administrator permissions to use the **Administrative Tools** and the administrator permissions you have determine what you can view and modify.

The navigation pane along the left side of the console gives you access to these administrative tools.

Table 14: Administrative Tools

Administrative Tools	Description	Administrator permissions
Toolbox	Where you can gain quick access to all the tasks you can perform from a single portal	Users with any Safeguard administrator privileges
Accounts	Where you associate account identities with managed systems	Asset Administrator or Auditor
Account Groups	Where you define sets of accounts that you can add to the scope of an access request policy	Auditor or Security Policy Administrator
Assets	Where you add computers, servers, network devices, or applications to be managed by a Safeguard for Privileged Passwords Appliance	Asset Administrator or Auditor
Asset Groups	Where you define sets of assets that you can add to the scope of an access request policy	Auditor or Security Policy Administrator

Administrative Tools	Description	Administrator permissions
Discovery	Where you configure asset and account discovery jobs which apply a set of rules to discover and automatically add assets and accounts to Safeguard for Privileged Passwords	Auditor or Asset Administrator
Entitlements	Where you specify the access request policies that restrict system access to authorized users	Auditor or Security Policy Administrator
Partitions	Where you define collections of assets that can be used to segregate assets for delegation	Asset Administrator, Auditor, or delegated partition owner
Settings	Where you configure Safeguard for Privileged Passwords to run backups, install updates, manage clusters, manage certificates, enable event notifications, configure external integration, define profile configurations settings, define user password rules, define discovery rules, and run troubleshooting tools.	Users with any Safeguard administrator privileges; however, the settings available depend on the administrative permissions assigned.
Users	Where you set up users who can log in to Safeguard for Privileged Passwords.	Bootstrap, Asset Administrator, Auditor, Authorizer Administrator, Help Desk Administrator, Security Policy Administrator, or User Administrator
User Groups	Where you define sets of Safeguard for Privileged Passwords users that you can add to an entitlement.	Bootstrap, Auditor, Authorizer Administrator, Security Policy Administrator, or User Administrator

All of the **Administrative Tools** views have the following components, except for the Toolbox and Settings:

- Toolbar options across the top of the view.
- Object list (left pane)
- Search box at the top of the object list.
- Details pane (right pane)

Toolbar options

The toolbar at the top of the views (except for the Toolbox and Settings), contain these options, depending on your Administrator permissions and the administrative tool you are in.

These buttons are available:

- **Apply** to apply the changes and keep the dialog open
- **OK** to apply the changes and close the dialog.
- **Cancel** to ignore any changes made, if any, and close the dialog.

Toolbar options include the following.

- **Add**: Add objects to the Safeguard for Privileged Passwords appliance.
- **Delete**: Remove objects from the appliance.
- **Refresh** the screen.

  NOTE: Whenever you add, modify, or delete an object in **Administrative Tools**, the changes you make cannot be seen by other administrators running Safeguard for Privileged Passwords on other clients unless they click **Refresh**.

- **Import** : Only available for Accounts, Assets, and Users. Add a set of objects from a .csv file. For more information, see Importing objects on page 462.
- **User Security**: Only available for Users. Menu options include **Set Password** and **Unlock** accounts. For more information about these options, refer to Setting a local user's password and Unlocking a user's account.
- **Account Security**: Only available for Accounts. Menu options include: **Set Password**, **Check Password**, and **Change Password**. For more information, see Checking, changing, or setting an account password on page 165.
- **Permissions**: Only available for Users. Set administrator permissions for users. For more information, see Administrator permissions on page 507.
- **Set as Default**: Only available for Partitions. Set a partition as the default. For more information, see Setting a default partition and Setting a default partition profile.
- **Download SSH Key**: Only available for Assets. Add the SSH Key to the selected asset. For more information, see Downloading a public SSH key on page 222.
- **Password Archive**: Only available for Accounts. Display the password history for the selected account. For more information, see Viewing password archive on page 166.
- **Access Requests**: Only available for Accounts and Assets. Enable or disable access request services for the selected account or asset.

- **Show Disabled**: Display the accounts or assets marked as disabled.
- **Hide Disabled**: Hide the accounts or assets marked as disabled.
- **Sync Now**: Only available for Assets. Run the directory addition and deletion synchronization process on demand. In addition, it runs through the discovery, if there are discovery rules and configurations set up.

10

Search box

Whether you are using the desktop client or web client, 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 selection 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: in the web client, the Approvals and Reviews searches are case sensitive.
- Wild cards are not 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 the Settings pane, 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 rules` to return **Safeguard Access** | **Password Rules**. If you enter **"password rules"** or **password_rules**, the following message is returned: `No matches found`.
    - On the Users pane search box:
        - A general search does not return anything if you use quotes because it uses a literal search (searches for the quotes). For example: searching for "ab_misc2" returns the message: `There is nothing to show here`.
        - 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.

- When you combine a basic 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 basic search must come after the attribute searches.
- In large environments, you will see a result number to tell you how many objects match the criteria; however, only the first 200 objects will be retrieved from the server. When you scroll down the list, more objects will be retrieved (paged) as needed.

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 ⊗ **Clear**.

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

You can also Search by attribute and Select a drop-down to sort .

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. 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.

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 **Clear**.

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

Attributes in each Search box

The following attributes are available when you click the icon. In addition, API attributes can be searched in the search box.

Accounts

- Name
- Description
- Asset
- Domain Name
- Profile
- Partition
- Tag

Account Groups

- Name
- Description
- Dynamic

Assets

- Name
- Description
- Platform
- Forest Root Domain
- Network Address
- Partition
- Is Directory
- Tag

Asset Groups

- Name
- Description

- Dynamic

Entitlements

- Priority
- Name
- Description
- Users Display Name
- Users Name

Partitions

- Name
- Description

Users

- User Name
- Description
- First Name
- Last Name
- Email Address
- Domain Name

User Groups

- Name
- Description

Select a drop-down to sort

By default, the desktop client lists the objects in alphabetical order; however, you can use the controls located above the list to sort the object list.

To sort the desktop client object lists

1. Select **Ascending** or **Descending** under the **Search** box to sort the list in either alphabetical or reverse-alphabetical order.
2. To sort the list of **Accounts**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
    - Name (Default)
    - Description

- Asset
- Domain Name
- Profile
- Partition

3. To sort the list of **Account Groups**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Dynamic
4. To sort the list of **Assets**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Platform
   - Network Address
   - Partition
5. To sort the list of **Asset Groups**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
   - Dynamic
6. To sort the list of **Entitlements**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Priority (Default)
   - Name
   - Description
7. To sort the list of **Partitions**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
   - Name (Default)
   - Description
8. To sort the list of **Users**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:

- User Name (Default)
- Description
- First Name
- Last Name
- Email Address
- Domain Name

9. To sort the list of **User Groups**, open the drop-down menu under the **Search** box and choose one of the following options before sorting the list in either **Ascending** or **Descending** order:
    - Name (Default)
    - Description
    - Type (Sorts by local and directory groups.)

11

Privileged access requests

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 in the desktop client or web client.

As a Safeguard for Privileged Passwords 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 118.

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 then appear on their **Home** page for subsequent use. This can be done from either the desktop client or web client:

  - Desktop client: For more information, see Desktop client favorite request on page 88.
  - Web client: For more information, see Favorites (web client) on page 76.
- Approvers see tasks related to approving (or denying) and revoking access requests.
- Designated reviewers see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

Password release and session requests use a workflow engine; however, the actions taken on a session request are slightly different than those taken on a password release request. Therefore, we will cover each of these access request workflows separately:

- Password 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.

- Access Request Approved
- Access Request Denied
- Access Request Expired
- Access Request Pending Approval
- Access Request Revoked
- Password was Changed
- Review Needed

Toast notifications may also appear on your console when the desktop client application is not the active foreground application.

Using the desktop client, there are two ways to configure Safeguard for Privileged Passwords to send event alerts to Safeguard for Privileged Passwords users:

- Toast notifications
- Email notifications

Toast notifications

Toast notifications are alerts that appear on your console when the desktop client application is not the active foreground application. For example, a toast notification may display when you are in another application or when you have minimized the Safeguard for Privileged Passwords desktop client.

(desktop client) To enable toast notifications

1. In the desktop client, open Settings (desktop client).
2. Select the **Enable Toast Notifications** check box.

NOTE: When you select the **Run in the System Tray** check box, you cannot modify the toast notifications option because in that mode, you always get notifications.

Email notifications

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

- You must set your email address correctly in the desktop client, **My Account**. For more information, see User information and log out (desktop client) on page 86.
- 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 on page 276.
- The Appliance Administrator must configure the SMTP server. For more information, see Enabling email notifications on page 396.

Role-based email notifications generated by default

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.

Table 15: Email notifications based on administrative permissions

Administrative permission	Event/Warning
Appliance Administrator Operations Administrator	Appliance Healthy Appliance Restarted Appliance Sick Appliance Task Failed Archive Task Failed Cluster Failover Started Cluster Replica Enrollment Completed Cluster Replica Removal Started Cluster Reset Started Disk Usage Warning Factory Reset Appliance License Expired License Expiring Soon NTP Error Detected Operational Mode Appliance Raid Error Detected Reboot Appliance Shutdown Appliance
Partition Owner (if none, sent to the Asset Administrator) NOTE: If Asset Administrators want to be notified	Account Discovery Failed Dependent Asset Update Failed Password Change Failed

Administrative permission	Event/Warning
along with the Partition Owners, they can set themselves up as an explicit owners or create an email subscription for the event (for example, `IsSystemOwned=false`). The API `/service/core/v3/EventSubscribers` endpoint can be used to create event subscribers for events, including events on specific assets or accounts.	Password Check Failed Password Check Mismatch Password Reset Needed Restore Account Failed Ssh Host Key Mismatch Ssh Key Change Failed Ssh Key Install Failed Suspend Account Failed Test Connection Failed
Security Policy Administrator	Policy Expiration Warning Policy Expired Entitlement Expiration Warning Entitlement Expired

NOTE: Safeguard for Privileged Passwords administrators can use the following API to turn off these built-in email notifications:

```
POST /service/core/v2/Me/Subscribers/{id}/Disable
```

In addition, Safeguard for Privileged Passwords administrators can subscribe to additional events based on their administrative permissions using the following API:

```
POST /service/core/v2/Events
```

Password release request workflow

Safeguard for Privileged Passwords provides secure control of administrative accounts by storing account passwords until they are needed, and releases them only to authorized persons. Then, Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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.

The following topics explain the entire end-to-end password release process from request to approval to review.

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 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 on page 118.

To request a password release

1. Go to the new access request page:

- (web client): Click **Home** or **My Requests**, then click **New Request**.
- (desktop client): Go to the **Home** 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 **Asset Selection**, select the assets to be included in the access request. The assets available for selection are based on the scope defined in the entitlement's access request policies. There is a limit of 50 assets.
3. On **Account & Access Type Selection**, select the accounts to be included in the access request and the type of access being requested for each selected account. The accounts include linked accounts, if any. For more information, see Linked Accounts tab (user) on page 448.
   - **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 hyperlink, multiple access request types are available. Select the hyperlink and select the access type.

   You can remove an asset or account from the list. Select the entry in the grid and click **Delete**.
4. On **Request Details**, configure the following settings, which will apply to all of the selected assets and accounts:

a. **Normal Access**: If the policy has emergency access enabled, select this option to gain normal access to this password. Normal access ensures the access request goes through the entire end-to-end access release process from request to approval to review as defined in the policy by the Security Policy Administrator.

b. **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 on page 276.

c. **Request Immediately**: If selected, the request is immediately created. You can clear this option to enter a specific date and time for the request in the user's local time.

d. **Checkout Duration**: 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 on page 276.

e. **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. This feature is set up through the desktop client.For more information, see Ticketing systems on page 417.

f. **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 312.

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

g. **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, click the **Add to Favorites** button.

   Add to Favorites displays, allowing you to specify a name and description for the access request. It also allows you to assign a color to the request's icon.

   This access request is then added to your **Favorites**. How you manage favorites depends on your interface:

   - In the web client, favorites are displayed on the **Home** page and the **My Requests** page. For more information, see Favorites (web client) on page 76.

- In the desktop client, select the favorite request from the **Favorites** pane. In the **New Access Request** dialog, you can edit the request details or enter a required reason or comment before submitting the request. For more information, see Desktop client favorite request on page 88.

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

   The **Results** dialog displays the access requests submitted and whether a request was successful.

When the request has been approved, you can use the password. For more information, see Taking action on a password release request on page 123.

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 and the client interface you are using.

(web client) 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 **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.
     - **All**: Requests in all states.
     - **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 Passwords 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 search-able elements. Or enter search characters. For more information, see Search box.

2. You can take any of the following actions on the password release request:

   - **Available** request: Make selections on the request based on your user interface.

- Click on to expand the box to see the options.
- If your browser allows, click **Copy** to check out the password. This puts the password into your copy buffer, 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. 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** to complete the password check out process.

- **Approved** request: Select **Cancel** 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** to remove the request.
- **Revoked** request: Select **Resubmit Request** to request the password again.

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

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

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

(desktop client) To take action on a password release request

1. From your **Home** page, the **Requests** widget has these controls:
   - Select (**expand down**) to open the list of active requests.
   - Select **Popout** to float the **Requests** pane. You can then select and drag the pane to any location on the console and re-size the window.Open the list of requests.

     NOTE: You enable or disable the **Home** page widgets in the Settings (desktop client) menu.

2. Open the list of requests and select one of the following view filters. The number indicates how many requests are in that state.
   - **All**: Requests in all states.
   - **Available**: Approved requests that are ready to view or copy.
   - **Approved**: Requests that have been approved, but the check out time has not arrived.

- **Pending**: Requests that are waiting for approval or for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
- **Revoked**: Approved requests retracted by the approver. The approver can revoke a request between the time the requester views the password and checks it in.
- **Expired**: Requests for which the **Checkout Duration** has elapsed.
- **Denied**: Requests denied by the approver.

3. Select an account to see the details of the password release request.
4. Take the following actions on password release requests:
   - **Available**: Make selections on the request based on your user interface.
     - Click **Copy** to check out the password. This puts the password into your copy buffer, 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. 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** to complete the password check out process.
   - **Approved**: Select **Cancel** 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**: Select **Cancel** to remove the request.
   - **Revoked**: Select **Resubmit Request** to request the password again.

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

     Select **Remove** 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 Safeguard for Privileged Passwords 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.

Safeguard for Privileged Passwords can be configured to notify you of a password release request that requires your approval. For more information, see Configuring alerts on page 118.

(web client) To approve or deny a password release request

If you are an approver, click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details: Select the request and the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click to approve all the selected requests. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click to deny all the selected requests. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see.
- Search: For more information, see Search box on page 111.

(desktop client) To approve or deny a password release request

1. From your **Home** page, the **Approvals** widget has these controls:
   a. Select (**expand down**) to open the list of approvals.
   b. Select **Popout** to float the **Approvals** pane.

      You can then select and drag the pane to any location on the console and re-size the window.

   NOTE: You enable or disable the **Home** page widgets in the Settings (desktop client) menu.
2. Open the list of approvals and select one of the following view filters. The number indicates how many requests are in that state.
   - **All**: Password release requests in all states.
   - **Pending**: Requests that are waiting for approval.
   - **Approved**: Requests that have been approved, but not yet available to the requester.
3. Once you open the list, select the requester's name to see the details of the password release request.
4. Take the following actions on password release requests:
   - **Pending**: Select to **Approve** or **Deny** a password release request. Optionally, enter a comment of up to 255 characters.

- **Pending Additional Approvers**: Select to **Deny** a password release request. Optionally, enter a comment of up to 255 characters.
- **Approved**: Select to **Deny** or **Revoke** an approved request.

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 Safeguard for Privileged Passwords to notify you of a password release request that requires your review. For more information, see Configuring alerts on page 118.

(web client) 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: Select the request and the details display on the right of the page.
- Mark one or more request as reviewed: Select the requests. Then, click **Mark all the selected requests as reviewed**. A comment may be required or, if not required, added.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
- Search: For more information, see Search box on page 111.

(desktop client) To review a completed password release request

1. From your **Home** page, the **Reviews** widget has these controls:
   a. Click (**expand down**) to open the list of pending reviews.
   b. Click **Popout** to float the **Reviews** pane.

      You can then select and drag the pane to any location on the console and re-size the window.

   NOTE: You enable or disable the **Home** page widgets in the Settings (desktop client) menu.
2. Open the list of pending reviews and select an account name to see the details of the password release request.
3. Take the following action on password release requests:
   - Select **Workflow** to review the transactions that took place in the selected request.

- Select **Review** to complete the review process.

  Optionally, enter a comment of up to 255 characters.

Once the review is complete, it no longer appears on the **Reviews** pane.

TIP: If one requester checks in the request and another requester wants to use it, the second requester is unable to check out the password until the original request has been reviewed. However, the Security Policy Administrator can **Close** a request that has not yet been reviewed. This will bypass the reviewer in the workflow and allow the account to be accessed by another requester.

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 terminate 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 Safeguard for Privileged Passwords 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.

The following topics explain the entire end-to-end session access process from request to approval to review (and play back if sessions recording is enabled).

About sessions and recordings

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 is included in the install. The desktop client looks for any user-installed PuTTY in the following locations:

- Any reference to putty in the PATH environment variable
- `c:/Program Files/Putty`
- `c:/Program Files(x86)/Putty`
- `c:/Putty`

If PuTTY is not found, the desktop client uses the version of PuTTY that it installed at:

`<user-home-dir>/AppData/Local/Safeguard/putty`.

If the user later installs PuTTY in any of the locations above, the desktop client uses that version which ensures the user has the latest version of PuTTY.

Important notes

- Sessions requests are enabled by default. However, if authorized users cannot request sessions, check the **Session Requests Enabled** setting in the desktop client (**Administrative Tools** | **Settings** | **Access Request** | **Enable or Disable Services**).

  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 Safeguard for Privileged Passwords detects no activity for 10 minutes during a privileged session, the session is terminated.

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 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 118.

To request session access

1. Go to the new access request page:
   - From the web client, click **Home** or **My Requests**, then click + **New Request**.
   - From the desktop client, go to the **Home** 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 **Asset Selection**, select the assets to be included in the access request. The

assets available for selection are based on the scope defined in the entitlement's access request policies. The limit is 50 assets.
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.

3. On **Account & Access Type Selection**, select the accounts to be included in the access request and the type of access being requested for each selected account. The accounts include linked accounts, if any. For more information, see Linked Accounts tab (user) on page 448.
   - **Asset**: The display name of the managed system.
   - **Network Address**: The network host name or IP address of the managed system.
   - **Account**: The accounts available appear 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.

     The accounts available for selection are based on the **Asset-Based Session Access** setting. For more information, see Access Config tab. Or, the accounts available for selection may have been added in the Scope tab when editing the entitlement access policy. For more information, see Scope tab.

     The settings are:
     - If **None** is selected in the access request policy, the accounts Safeguard for Privileged Passwords retrieved from the vault will be available for selection. The selected account will then be used when the session is requested.
     - If **User Supplied** is selected in the access request policy, you will be required to enter the user credentials as part of the request workflow, prior to launching the SSH, RDP, or telnet session.
     - If **Linked Account** is selected in the access request policy, linked directory accounts will be available for selection. The selected account will then be used when the session is requested.
     - If **Directory Account** is selected in the access request policy, only the specified directory accounts will be available for selection. The selected directory account will then be used when the session is requested.
   - **Domain**: The name of the domain for the request.
   - **Access Type**: The type of access request appears in the **Access Type** column. When multiple access request types are available, this value appears as a hyperlink, which when selected displays an additional dialog allowing you to select the access type. Select one of the following for a session request: **RDP**, **SSH**, or **Telnet**.

The access type options available depend on the type of asset selected on **Asset Selection**. For example, RDP is only available for Windows sessions.

You can remove an asset or account from the list, select the entry and click **− Delete**.

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

   a. **Normal Access**: If the policy has emergency access enabled, select this option to gain normal access to this password. Normal access ensures the access request goes through the entire end-to-end access release process from request to approval to review as defined in the policy by the Security Policy Administrator.

   b. **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 on page 276.

   c. **Request Immediately**: Clear this option to enter a specific date and time for the request. Enter the time in the user's local time.

   d. **Checkout Duration**: This either displays the **Checkout Duration**; or, if the **Allow Requester to Change Duration** option is enabled in the policy, it allows you to set the days, hours, and minutes that you want the password and overrides the **Checkout Duration** set in the access request policy. For more information, see Creating an access request policy on page 276.

   e. **Ticket Number**: If the policy requires a ticket number, enter a valid ticket number for this request. When multiple accounts are specified in the request, if any of the selected accounts require a ticket number, you must specify a valid ticket number. The specified ticket number will be applied to all of the requests associated with this access request. This feature is set up through the desktop client. For more information, see Ticketing systems on page 417.

   f. **Reason**: If the policy requires reason, select an access request reason code for this request. Select the **Description** down arrow to view the description defined for the selected reason. When multiple accounts are specified in the request, if any of the selected accounts require a reason, you must specify a reason. The specified reason will be applied to all of the requests associated with this access request. For more information, see Reasons on page 312.

   g. **Comment**: 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, click the **Add to Favorites** button.

   Add to Favorites displays, allowing you to specify a name and description for the access request. It also allows you to assign a color to the request's icon.

   This access request is then added to your **Favorites**. How you manage favorites depends on your interface:

- In the web client, favorites are displayed on the **Home** page and the **My Requests** page. For more information, see Favorites (web client) on page 76.
- In the desktop client, select the favorite request from the **Favorites** pane. In the **New Access Request** dialog, you can edit the request details or enter a required reason or comment before submitting the request. For more information, see Desktop client favorite request on page 88.

6. After entering the required information, click **Submit Request**. **Access Request Result** displays showing you the access requests submitted and whether a request was successful.

7. To copy or view information, click the (**expand down**) arrow on the left of an active request.
   - If the access request is for sessions:
     - Click **Copy** to copy the connection string to the clipboard. Paste the string into a client application to launch the session.
     - Click **Show** to view the connection string.
     - Click **Help** to copy the value into the appropriate field of the configuration dialog.
   - If the access request is for passwords:
     - Click **Copy** to copy credential to the clipboard. The credential can then be pasted into the dialog that needs the credential to grant access.
     - Click **Show** to view the credential.
     - Click **Help** to copy the value into the appropriate field of the configuration dialog.

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 SPS. Try again so the request can be redirected to another managed host in the SPS cluster.
  - The SPS configuration is locked. Try again because this condition is typically because the SPS administrator is making configuration changes to the SPS 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 desktop client, go to **Entitlements** | **Access Request Policy** | **Sessions Settings** to add a valid connection policy.

Save the policy and recreate the access request. For more information, see Session Settings tab.

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 and the client interface you are using.

(web client) 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 111.
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 terminated.
   - **Expired**: Requests for which the **Checkout Duration** has elapsed.
   - **Denied**: Requests denied by the approver.
4. Click or to see more or less information on the request.
5. You can take the following actions on session requests, depending on the state.
   - **Available**: 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, if enabled by your Administrator. **Seconds Remaining** shows you how long you have to copy information to use to log in.
     - For SSH and RDP accounts:
       - Click **Launch** 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. 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 SPS 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** to complete the password check out process. This makes the session request available to reviewers.
  - Click **Hide** to conceal the information from view.

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

(desktop client) To take action on a session request

1. From your **Home** page, use any of these controls on the **Requests** widget, as needed. You can enable or disable the **Home** page widgets in the Settings (desktop client) menu.
   - Select (**expand down**) to open the list of active requests.
   - Select **Popout**. You can then select and drag the pane to any location on the console and re-size the window to float the **Requests** pane.
2. Open the list of requests and select one of these view filters. The number indicates how many requests are in that state.
   - **All**: Requests in all states
   - **Available**: Approved requests that are ready (that is, a session that can be launched)
   - **Approved**: Requests that have been approved, but the check out time has not arrived
   - **Pending Approval**: Requests that are waiting for approval
   - **Revoked**: Approved requests retracted by the approver
     - The approver can revoke a request between the time the requester launches the session and checks it back in.
     - When a user with Security Policy Administrator permissions revokes a live session, the active session is terminated.
   - **Expired**: Requests for which the **Checkout Duration** has elapsed.
   - **Denied**: Requests denied by the approver.
3. Select an account to see the details of the session request.
4. You can take the following actions on session requests, depending on the state.
   - **Available**: 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, if enabled by your Administrator. **Seconds Remaining** shows you how long you have to copy information to use to log in.
     - For SSH and RDP accounts:
       - Click **Launch** 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 outprocess 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.
        - Click **Help** to copy the value into the appropriate field of the configuration dialog.
    - 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. 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 SPS 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** to complete the password check out process. This makes the session request available to reviewers.
        - Click **Hide** to conceal the information from view.
- **Approved**: Select **Cancel** 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 Approval**: Click **Cancel** to remove the request.
- **Revoked**:
    - Click **Resubmit Request** to request the password again.
    - Click **Remove** to delete the request from the list.
- **Expired**: Click **Remove** to delete the request from the list.
- **Denied**:
    - Click **Resubmit Request** to request the password again.
    - Click **Remove** 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 Safeguard for Privileged Passwords users, or be auto-approved.

You can configure Safeguard for Privileged Passwords to notify you of an access request that requires your approval. For more information, see Configuring alerts on page 118.

(web client) To approve or deny a session request

If you are an approver, click **Approvals** on the left of the page to manage approvals. On the **Approvals** page, you can:

- View details: Select the request and the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click to approve all the selected requests. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click to deny all the selected requests. Optionally, enter a comment.
- Change the columns that display: Click and select the columns you want to see.
- Search: For more information, see Search box on page 111.

(desktop client) To approve or deny a sessions request

1. From your **Home** page, the **Approvals** widget has these controls:
   a. Select (**expand down**) to open the list of approvals.
   b. Select **Popout** to float the **Approvals** pane.

      You can then select and drag the pane to any location on the console and re-size the window.

   NOTE: You enable or disable the **Home** page widgets in the Settings (desktop client) menu.
2. Open the list of approvals and select one of these view filters:

State	Description
All	Requests in all states
Pending	Requests that are waiting for approval
Approved	Requests that have been approved, but not yet available to the requester

NOTE: The number indicates how many requests are in that state.

3. Once you open the list, select the requester's name to see the details of the sessions request.
4. Take the following actions on sessions requests:

State	Actions
Pending	Select to **Approve** or **Deny** a sessions request. Optionally, enter a comment of up to 255 characters.
Pending Additional Approvers	Select to **Deny** a sessions request. Optionally, enter a comment of up to 255 characters.
Approved	Select to **Deny** or **Revoke** an approved request. You can revoke a request between the time the requester views it and checks it in. Any eligible approver can deny an access request after it has already been approved or auto-approved. Once disallowed, the requester will no longer be able to access the requested session, but they are given another opportunity to request that session again. The requester receives an email notifying them that the request was denied. For more information, see Configuring alerts on page 118.

Launching the SSH client

Once an SSH session request becomes available, the requester can launch the SSH client to start the session. This is applicable for both the web client and desktop client user interfaces.

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 ▶ **Launch** button to the right of the asset name.
   - In the web client, a session will launch if you have an application registered (`ssh://` for SSH protocol).
   - In the desktop client, clicking ▶ **Launch** displays the **PuTTY Configuration** dialog. The required information is populated, click **Open** to launch the SSH client. If the required information is not populated in the **PuTTY Configuration** dialog, use the following buttons to copy and paste the information into the dialog:

- Use the buttons to the right of the **Hostname Connection String** to perform the following tasks:
  - **View**: To view the hostname connection string
  - **Copy**: To copy the value to your copy buffer, which can then be pasted into the Hostname field of the **PuTTY Configuration** dialog
  - **Help**: To copy the value into the Hostname field of the PuTTY Configuration dialog
- Use the buttons to the right of the **Password** to perform the following tasks.
  - **View**: To view the password
  - **Copy**: To copy the password to your copy buffer, which can then be pasted into the Password field of the **PuTTY Configuration** dialog
  - **Help**: To copy the value into the Password field of the **PuTTY Configuration** dialog

    NOTE: The Password field only appears if the **Include password release with session requests** option (Access Config tab) is selected in the entitlement's access request policy.

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 terminated. 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.

   This makes the session request available to reviewers. If the **Record Sessions** option is enabled in the policy, the reviewer can play back the recording as part of the review process. In addition, if the **Enable Command Detection** option is selected in the policy, the reviewer can view a list of the commands and programs run during the session.

Launching an RDP session

Once an RDP session request becomes available, the requester can launch the remote desktop connection to start the session. This is applicable for both the web client and desktop client user interfaces.

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. Depending on your interface:

   - (desktop client) Click the ▶ **Launch** button to the right of the asset name. Clicking this button displays the **Remote Desktop Connection** dialog. Click **Connect** to launch the remote desktop session.

   - (web client) In the web client:

     - If you have an application registered (`rdp://` for RDP sessions), you can click the ▶ **Launch** button to the right of 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 ▶ **Launch** button. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.

   NOTE: If the required information is not populated in the **Remote Desktop Connection** dialog, use the following buttons to copy and paste the information into the dialog:

   1. Use the buttons to the right of the **Username Connection String** to perform the following tasks:

      - **View**: To view the username connection string.

      - **Copy**: To copy the value to your copy buffer, which can then be pasted into the Username field of the **Remote Desktop Connection** dialog.

      - **Help**: To copy the value into the Username field of the **Remote Desktop Connection** dialog.

   2. Use the buttons to the right of the **Password** to perform the following tasks:

      - **View**: To view the password.

      - **Copy**: To copy the password to your copy buffer, which can then be pasted into the Password field of the **Remote Desktop Connection** dialog.

      - **Help**: To copy the value into the Password field of the **Remote Desktop Connection** dialog.

      NOTE: The Password field only appears if the **Include password release with session requests** option (Access Config tab) is selected in the entitlement's access request policy.

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 terminated. 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.

This makes the session request available to reviewers. If the **Record Sessions** option is enabled in the policy, the reviewer can play back the recording as part of the review process. In addition, if the **Enable Window Title Detection** option is selected in the policy, the reviewer can view a list of the windows opened on the desktop during the 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 Safeguard for Privileged Passwords to notify you of an access request that requires your review. For more information, see Configuring alerts on page 118.

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*.

(web client) 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: Select the request and the details display on the right of the page.
- Mark one or more request as reviewed: Select the requests. Then, click **Mark all the selected requests as reviewed**. A comment may be required or, if not required, added.
- Change the columns that display: Click **Select columns to display** then select the columns you want to see.
- Search: For more information, see Search box on page 111.

(desktop client) To review a completed sessions request

1. From your **Home** page, the **Reviews** widget has these controls:
   a. Click (**expand down**) to open the list of pending reviews.
   b. Click **Popout** to float the **Reviews** pane.

      You can then select and drag the pane to any location on the console and re-size the window.

   NOTE: You enable or disable the **Home** page widgets in the Settings (desktop client) menu.

2. Open the list of pending reviews and select an account name to see the details of the sessions request.
3. Take the following action on sessions requests:
   a. Select **Workflow** to review the transactions that took place in the selected request.
      - If **Record Sessions** is enabled in the policy, click **Play** on the Initialize Session event to play back the session.

        A (green dot) indicates the session is live. A user with Security Policy Administrator permissions can click this icon to follow an active session.

        If the session recording has been archived from the local Safeguard file system or was recorded prior to joining a Sessions Appliance, you will see a **Download** button instead of a **Play** button. Click **Download** to download the recording and then click **Play**.

        > **CAUTION: If you receive a message like:** `No Desktop Player. The Safeguard Desktop Player is not installed. Would you like to install it now?`**, click Yes. See Installing the desktop client, Installing the Desktop Player, step 2.**

      - If **Enable Command Detection** is enabled in the policy, expand to show the details and click the **events** link on the Initialize Session event to view a list of the commands and programs run during the session.

        For an RDP session, the setting is **Enable Windows Title Detection**. When enabled, you can view a list of windows that were opened during the privileged session.
   b. Select **Review** to complete the review process.

      Optionally, enter a comment of up to 255 characters.

   Once the review is complete, it no longer appears on the Reviews pane.

Replaying a session

You can play back a recorded session from the **Request Workflow** dialog, which can be accessed by clicking the **Workflow** button that appears to reviewers for completed session requests and in the Activity Center view when an access request event is selected in an activity audit log report. In addition, you can play back a recorded session by clicking the icon displayed to the left of an access request session event on the activity audit log report in the Activity Center view.

> NOTE: This feature is only available for session requests that have **Record Session** enabled in the access request policy (**Access Config** tab).

(desktop client only) To play back a session (Request Workflow dialog)

1. Open the **Request Workflow** dialog using the **Workflow** button.

   NOTE: If accessing the **Request Workflow** dialog from the Activity Center, select an **Access Request Session** event from the activity audit log report.

2. Locate an Initialize Session event and click ▶ **Play** to launch the Desktop Player.

   A ● (green dot) indicates the session is live. A user with Security Policy Administrator permissions can click this icon to follow an active session.

   If the session recording has been archived from the local Safeguard file system, you will see a **Download** button instead of a ▶ **Play** button. Click **Download** to download the recording and then click ▶ **Play**.

   CAUTION: If you receive a message like: `No Desktop Player. The Safeguard Desktop Player is not installed. would you like to install it now?`**, click Yes. See Installing the desktop client, Installing the Desktop Player, step 2.**

3. Accept the certificate to continue.

   In the Certificate error message, click **Continue** to use the default Session Recording Signing certificate shipped with Safeguard for Privileged Passwords. To use a different SSL certificate, click **Abort** and then import the appropriate certificates including the root CA.

4. Use one of the following methods to play back the session recording:
   - Click ▶**Play Channel** from the toolbar at the top of the player.
   - Click ▶ in the thumbnail in the upper right corner of the Information page.
   - Click ▶**Play Channel** next to a channel in the Channels pane.

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*.

Following and terminating a "live" session

An access request session event with a ● (green dot) in the left-most column of the activity audit log report or **Request Workflow** dialog indicates that the session is "live". Clicking this button launches the Desktop Player allowing you to follow what is happening in the active session. Safeguard for Privileged Passwords also allows you to terminate an active session directly from the desktop player.

NOTE: You must have Security Policy Administrator permissions to follow an active session.

(desktop client only) To watch or terminate a "live" session

1. From the **Request Workflow** dialog or Activity Center activity audit log report click the ● (green dot) next to an access request session event.

   NOTE: Security Policy Administrators can also launch the Safeguard Desktop Player from the Access Requests view. Select an access request session in the request grid and click the **View Live Session** toolbar button.

   The Safeguard Desktop Player launches allowing you to watch the active session. On the Information page, the thumbnail (upper right) displays a blinking red recording button when a session is "live".

2. Use one of the following methods to follow the session:
   - Click ▶**Play Channel** from the toolbar at the top of the player.
   - Click ▶ in the thumbnail in the upper right corner of the Information page.
   - Click ▶**Play Channel** next to a channel in the Channels pane.
3. In the play back window, you will see a **Terminate** button and a **Live** indicator in the lower right corner.
4. Click **Terminate** to stop the active session.

NOTE: You can also terminate an active session by revoking the session through the Windows desktop client.

12

Toolbox

When you select the **Administrative Tools** link from the **Home** page navigation pane, the **Toolbox** view appears. This view gives you quick-start links to the tasks you can perform.

NOTE: The display is tailored to your Administrator permissions.

Each numbered tile gives you quick access to its **Administrative Tool**. Clicking **+** displays the dialog allowing you to add an object.

In addition, the Toolbox allows you to view the status of running tasks.

- Viewing task status
- Stopping a task

Viewing task status

Safeguard for Privileged Passwords displays a number on your **Toolbox** navigation link to notify you when you have any tasks running.

To view task status

1. Navigate to the **Toolbox**.
2. Click **Popout** to float the **Tasks** pane.

   You can then select and drag the pane to any location on the console and re-size the window.
3. Click **Remove** to delete a task from the pane.
4. Click **Cancel** next to a running task to stop a task.
5. Click **Clear** to remove all items from the **Tasks** pane.

Stopping a task

To stop a task

1. In the **Toolbox**, open the **Tasks** pane.
2. Click ⊗ **Cancel** next to a running task.

13

Accounts

A Safeguard for Privileged Passwords account is a unique identifier that Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords 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 on page 201.

The **Accounts** view displays the following information about the selected account.

- General tab (account): Displays general information about the selected account.
- Access Request Policies tab (account): Displays the entitlements and access request policies associated with the selected account.
- Account Groups tab (account): Displays the account groups that contain the selected account.
- Dependent Assets (account): Displays the assets that have dependency on the selected directory account.
- Check and Change Log tab (account): Displays the password validation and reset history for the selected account.
- History tab (account): Displays the details of each operation that has affected the selected account.

For information about configuring Account Discovery in Safeguard for Privileged Passwords, see Account Discovery job workflow.

Use these toolbar buttons to manage accounts.

- **Add Account**: Add accounts to Safeguard for Privileged Passwords. For more information, see Adding an account on page 156.
- **Delete Selected**: Remove the selected account. For more information, see Deleting an account on page 160.

- **Refresh**: Update the list of accounts.
- **Import Accounts**: Add accounts to Safeguard for Privileged Passwords. For more information, see Importing objects on page 462.
- **Account Security**: Menu options include **Check Password**, **Change Password**, and **Set Password**. For more information, see Checking, changing, or setting an account password on page 165.
- **Password Archive**: Display the password history for the selected account. For more information, see Viewing password archive on page 166.
- **Access Requests**: 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
  - **Show Disabled**: Display the accounts that are not managed and are disabled and have no associated assets. Account management can be controlled by right clicking on an asset and selecting **Enable-Disable**.
  - **Hide Disabled**: Hide the accounts that are not managed and are disabled and have no associated assets. Asset management can be controlled by right clicking on an account and selecting **Enable-Disable**.
- **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 111.

General tab (account)

The **General** tab lists information about the selected account.

Large tiles at the top of the tab display the number of **Access Request Policies**, **Account Groups**, and **Dependent Assets** associated with the selected account. Clicking a tile heading opens the corresponding tab. The time stamps for the password and SSH key check and change transactions are based on the user's local time.

Navigate to **Administrative Tools** | **Accounts** | **General**. Information for the account displays. Not all the information listed below is applicable for every account.

Table 16: Accounts General tab: General properties

Property	Description
Name	The name of the selected account.
Distinguished Name	For LDAP platforms, the fully qualified distinguished name (FQDN) for the service account
Domain Name (for directories)	The name of the domain where the account was discovered
SID (for directories)	Security IDentifer for a Windows account.
Asset	The display name of the managed system associated with this account. Accounts are only associated with one asset.
Partition	The name of the partition where the selected account resides.
Profile	The name of the profile that governs the accounts assigned to a partition.
Password Sync Group	If assigned, the password sync group to control password validation and reset across all associated accounts.
Account Discovery Job	The account discovery job with rule-based settings to discover all accounts that are assigned to the assets in a selected partition, that are made available globally, or that meet the rules criteria.
Date/Time Discovered	The date and time when the account was discovered.
Discovered User ID	The User ID of the discovered account.
Discovered Groups (for directories)	The groups in which the account is a member. Click the link to go to the **Discovered groups** dialog to view the groups.
Enable Password Request	True or False, indicating whether password release requests are enabled for this account.
Enable Session Request	True or False, indicating whether session access requests are enabled for this account.
Available for use across all partitions (Global Access for directories)	When selected, any partition is able to use this account and the password is given to other administrators. For more information, see Adding an Account Discovery rule on page 254.
Last Successful Password Check	The date and time of the last successful password validation.
Password Check Failures	Displays the number of password check tasks that failed.
Next Password	The date and time of the next automated password check as set in

Property	Description
Check	the **Check Password** schedule of the partition profile. For more information, see Adding check password settings on page 430.
Last Successful Password Change	The date and time of the last successful password change.
Next Password Change	The date and time of the next automated password change as set in the **Change Password** schedule of the partition profile. For more information, see Adding change password settings on page 426.
Password Change Failures	Displays the number of password change tasks that failed.
Last Successful SSH Key Change	The date and time of the last successful SSH key change.
SSH Key Change Failures	Displays the number of SSH key change tasks that failed.
Next SSH Key Change	The date and time of the next SSH key change.

Tags: Tag assignments for the selected account.

The tiles displayed in the **Tags** pane include 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.

> NOTE: Dynamically assigned tags contain a lightening bolt icon and cannot be deleted. Static tags which can be removed contain an X icon.

Description: Information about selected account.

Related Topics

Modifying an account

Access Request Policies tab (account)

The **Access Request Policies** tab displays the entitlements and access request policies, including password release policies and session request policies, associated with the selected account.

Navigate to **Administrative Tools** | **Accounts** | **Access Request Policies**.

Table 17: 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.

Use these buttons on the details toolbar to manage your access request policies associated with the selected account.

Table 18: 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 access request policies.
Details	View and edit details about the selected access request policy. For more information, see Creating an access request policy.
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 111.

Account Groups tab (account)

The **Account Groups** tab displays the account groups that contain the selected account. The **Account Groups** tab is only available to a user with Auditor permissions.

Navigate to **Administrative Tools** | **Accounts** | **Access Request Policies**.

Click **+ Add Account Group** from the details toolbar to add the selected account to one or more account groups.

Table 19: Accounts: Account Groups tab properties

Property	Description
Name	The account group name.
Dynamic	A check mark in this column indicates that the group is a dynamic account group.
Description	Information about the account group.

Use these buttons on the details toolbar to manage the account groups.

Table 20: Accounts: Access Request Policies tab toolbar

Option	Description
Add Account Group	Add the selected account an account group.
Remove Selected	Remove the selected account group from the account.
Refresh	Update the list of account groups assigned to the selected account.
Search	To locate a specific account group in this list, enter the character string to be used to search for a match. For more information, see Search box on page 111.

Related Topics

Adding an account to one or more account groups

Dependent Assets (account)

The **Dependent Assets** tab only displays for a directory asset and displays the assets that have dependency on the selected directory account. Dependencies are created via **Administrative Tools** | **Assets**, **Account Dependencies** tab, then **Add Account**. For more information, see Adding account dependencies on page 216.

Navigate to **Administrative Tools** | **Accounts** | **Dependent Assets**.

Table 21: Accounts: Dependent Assets tab properties

Property	Description
Name	The Windows asset name

Property	Description
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 22: Accounts: Access Request Policies 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 Search box on page 111.

Check and Change Log tab (account)

The **Check and Change Log** tab displays the password validation and reset history for the selected account.

Time Frame: By default, the check and change log entries displayed are for the last 24 hours. Click one of the time intervals at the top of the grid to display log entries for a different time frame. If the display does not refresh after selecting a different time interval, click the **Refresh**.

Click **+ Add Account Group** from the details toolbar to add the selected account to one or more account groups.

Navigate to **Administrative Tools** | **Accounts** | **Check and Change Log**.

Table 23: Accounts: Check and Change Log tab properties

Property	Description
User	The display name of the user that triggered the event
Status	The status of the transaction: • Failure • Success • Queued
Reason	A system message pertaining to the password validation and reset activity, such as the password matches the asset, was changed

Property	Description
	successfully, or does not match the asset.
Type	The type of transaction: • Check Password • Change Password NOTE: **Check and Change Log** only displays events that the appliance performs; that is, it only displays Check Password and Change Password transactions. It does not display Set Password transactions. For more information, see Checking, changing, or setting an account password on page 165.
Date	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.

History tab (account)

The **History** tab allows you to view or export the details of each operation that has affected the selected account.

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.
- **Search**: For more information, see Search box on page 111.
- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Navigate to **Administrative Tools** | **Accounts** | **History**.

Table 24: 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

Property	Description
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
Parent	The name of the object to which the selected account is a child
Parent Object Type	The parent object type

Select an event to display this additional information for some types of events (for example, create and update events).

Table 25: Additional History tab properties

Property	Description
Property	The property that was updated
Old Value	The value of the property before it was updated
New Value	The new value of the property

Managing accounts

Use the controls and tabbed pages on the Accounts page to perform the following tasks to manage Safeguard for Privileged Passwords accounts:

- Adding an account
- Adding a cloud platform account
- Manually adding a tag to an account
- Adding an account to one or more account groups
- Modifying an account

- Deleting an account
- Importing objects
- Checking, changing, or setting an account password
- Viewing password archive

Adding an account

It is the responsibility of the Asset Administrator to add assets and accounts to Safeguard for Privileged Passwords. 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: Safeguard for Privileged Passwords allows you to set up account discovery jobs that run automatically. For more information, see Account Discovery job workflow on page 251.

To add an account

1. Navigate to **Administrative Tools** | **Accounts**.
2. Click **+ Add Account** from the toolbar.
3. In the **Assets** dialog, for **Asset Name**, select an asset to associate with this account.
4. In the **Account** dialog, 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.
    - **Profile**: **Browse** to select a partition profile to govern this account.

      By default an account inherits the partition 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 profile on page 305.
    - **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 he or she is an authorized user.

- (For directory accounts only) **Available for use across all partitions**: 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.

Related Topics

Checking, changing, or setting an account password

Assigning assets or accounts to a profile

Account Discovery job workflow

Adding a cloud platform account

Adding a cloud platform account

Safeguard for Privileged Passwords can manage cloud platform accounts such as Amazon Web Services (AWS), Facebook (deprecated), and Twitter (deprecated).

Before you add cloud platform accounts to Safeguard for Privileged Passwords, you must first add an asset with which to associate the accounts. For more information, see Prepare Amazon Web Services platforms.

To add a cloud platform to Safeguard for Privileged Passwords

1. log in to Safeguard for Privileged Passwords and navigate to **Administrative Tools**.
2. In **Assets**, click **+ Add 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.
   c. **Partition**: Select the partition you want Safeguard for Privileged Passwords to use to manage the cloud platform account passwords.
   d. **Profile**: Select the profile you want Safeguard for Privileged Passwords to use to manage the cloud platform account passwords.
4. In the **Management** tab:

a. **Product**: Select the appropriate product, such as **Amazon Web Services**.

b. **Version**: For **Amazon Web Services**, select the version.

c. **Network Address**: For **Amazon Web Services**, enter the AWS Account ID or Alias which can be found on the AWS IAM User's view.

5. For **Amazon Web Services**, in the **Connection** tab, select:

   a. **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.

   -OR-

   b. **None** to not authenticate to the asset and manually manage the asset.

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 **+ Add Account** from the details toolbar.
3. In the **User Name** field, enter the cloud platform account username, email address, or phone number.
4. In the **Password** field, enter the account password for the user name you provided.
5. Click **Test Connection** to verify that Safeguard for Privileged Passwords can communicate with this cloud platform using the credentials that you have provided.
6. (Optional) Enter a **Description**.
7. **Browse** to select a profile to govern this account
8. Ensure the **Enable Password Request** option is checked and click **Add Account**.

Now you can manually check, change, or set the cloud platform account password; and, Safeguard for Privileged Passwords 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 341.

To manually add a tag to an account

1. Navigate to **Administrative Tools** | **Accounts**.
2. Select an account from the object list (left-pane).
3. Open the **General** tab and scroll down to view the **Tags** pane.
4. Click ✎ next to the **Tags** title. Existing tags are displayed.
5. Place your cursor in the edit box and use one method:
   - Enter the name of a tag.
   - Start entering the name of the tag. As you type, existing tags that start with the letters entered appear. Select from the list.
   - To add additional tags, press **Enter** before entering the next tag.
6. Click **OK**. If you do not see the new tag, click the **Refresh** toolbar button.
7. To remove a manually assigned tag, click ✎ next to the **Tags** title and click the **X** inside the tag box to be removed.

Adding an account to one or more account groups

From the **Accounts** view you can add an account to one or more account groups.

Select an account group to add to an account

1. Navigate to **Administrative Tools** | **Accounts**.
2. In **Accounts**, select an account from the object list and open the **Account Groups** tab.
3. Click **+ Add Account Group** from the details toolbar.
4. Select one or more account groups from the list in the **Account Groups** dialog and click **OK**.

Create an account group to add to an account

If you do not see the account group you are looking for and you have Security Policy Administrator permissions, you can create an account group from the **Account Groups**

dialog.

1. Click **+ Create New** and 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
2. Click **Add Account Group**.
3. Create additional account groups, as required.
4. Click **OK** in the **Account Groups** selection dialog to add the new account groups to the selected account.

Related Topics

Adding one or more accounts to an account group

Modifying an account

Once you add an account, you cannot modify an account's associated asset or its name, but you can modify other information.

To modify an account's information

Navigate to **Administrative Tools** | **Accounts**.

- To change the description, profile, or request settings, double-click the account from the object list.
- To view the selected account's password validation and reset history, switch to the **Check and Change Log** tab.
- To view or export the details of each operation that has affected the selected account, switch to the **History** tab. To export, select the time frame, then click **Export**.
- To reset an account's password, right-click the account name and navigate to **Account Security** and select to check, change, or set the password. For more information, see Checking, changing, or setting an account password on page 165.

Deleting an account

When you delete an account, Safeguard for Privileged Passwords does not delete it from its associated asset; it simply removes it from Safeguard for Privileged Passwords.

If you delete a service account, Safeguard for Privileged Passwords changes the asset's authentication type to **None**, which disables automatic password 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 for the accounts associated with it. For more information, see About service accounts on page 201.

To delete an account

1. Navigate to **Administrative Tools** | **Accounts**.
2. In **Accounts**, select an account from the object list
3. Click **Delete Selected**.
4. Confirm your request.

Importing objects

Safeguard for Privileged Passwords 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. For more information, see Creating an import file on page 164.

Once an import is completed, you can navigate to the **Tasks** pane in the Toolbox for details about the import process and invalid data messages. For more information, see Viewing task status on page 145.

To import objects

1. In **Administrative Tools**, click **Assets**, **Accounts**, or **Users** based on what data you are importing.
2. Click **Import** from the toolbar.
3. In the **Import** dialog, **Browse** to select an existing .csv file containing a list of objects to import.
4. When importing assets, the **Discover SSH Host Keys** option is selected by default indicating that Safeguard will retrieve the required SSH host key for the assets specified in the .csv file.
5. Click **OK**.

   Safeguard for Privileged Passwords imports the objects into its database.

   NOTE: Safeguard for Privileged Passwords does not add an object if any column contains invalid data in the .csv file, with the following exceptions:

   - Assets **PlatformDisplayName** property:
     1. If Safeguard for Privileged Passwords does not find an exact match, it looks for a partial match. If it finds a partial match, it supplies the ***<platform>*** **Other** platform, such as **Other Linux**.
     2. If it does not find a partial match, it supplies the **Other** platform type.
   - Users **TimeZoneId** property:
     1. If Safeguard for Privileged Passwords does not find a valid TimeZoneId property (that is, does not find an exact match or no time zone was

provided), it uses the local workstation's current time zone.

NOTE: Do not enter numbers or abbreviations for the TimeZoneId.

- Users **Password** property:
  1. Safeguard for Privileged Passwords adds a user without validating the password you provide.

Details for importing directory assets, service accounts, users, and user groups

You can use the steps like those above to import your existing directory infrastructure (such as Microsoft Active Directory). Managed account users cannot be members of the Protected Users AD Security Group.

Additional information specific to directory import follows.

1. Import the directory (and service account) via **Administrative Tools** | **Assets** | **Import Asset** and browse to select the .csv file. Safeguard for Privileged Passwords imports the directory as an asset.

   The directory's service account is automatically added to the list of accounts you can viewed via the **Assets** | **Accounts** tab.

   - By default, the service account password is automatically managed according to the check and change settings in the profile that governs the partition. For more information, see Creating a profile on page 302. If you do not want Safeguard for Privileged Passwords to manage the service account password, assign the account to a profile that is set to never change passwords. For more information, see Assigning assets or accounts to a profile on page 305.
   - The service account is added to the asset's Accounts tab and is disabled for password request and session request. For more information, see Accounts tab (asset) on page 186.
   - To change either setting, navigate to **Administrative Tools** | **Accounts** and double-click the account. Then select the following check boxes, as desired: **Enable Password Request** and **Enable Session Request**. For more information, see General tab (account) on page 148.
2. Import users and user groups.

   a. Import directory users via **Administrative Tools** | **Users** | **Import Users** and browse to select the .csv file.

   b. Assign to user groups via **Administrative Tools** | **Users Groups** | **Users** (select one or multiple users).

   c. Automatic synchronization: Once you import directory users and directory groups, Safeguard for Privileged Passwords automatically synchronizes the objects in its database with the directory schema attributes. User and group membership changes in the directory are reflected in Safeguard for Privileged Passwords. Directory users authenticate to Safeguard for Privileged Passwords with their directory credentials.

Active Directory and LDAP synchronization

Active Directory and LDAP data is automatically synchronized by asset or identity and authentication providers schema as shown in the following lists.

Asset schema list

- Users
  - Username
  - Password (modifiable in LDAP and not modifiable in Active Directory)
  - Description
- Groups
  - Name
  - Member
- Computer
  - Name
  - Network Address
  - Operating System
  - Operating System Version
  - Description

Identity and Authentication Providers schema list

- Users
  - Username
  - First Name
  - Last Name
  - Work Phone
  - Mobile Phone
  - Email
  - Description
  - External Federation Authentication
  - Radius Authentication
  - Managed Objects
- Groups
  - Name
  - Members
  - Description

Creating an import file

When importing objects, such as accounts, assets, or users, Safeguard for Privileged Passwords 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 **CSV Template Assistant**.
2. Select specific template properties from the template properties table, or select the **select all** check box in the heading. Safeguard for Privileged Passwords preselects the required properties; you can select any additional properties you desire.
3. Select **Download Template** to save a copy of the template properties table to a location of your choice.
   - Click the **View** icon in the Values column to display a list of allowable values. Click **Copy** to copy the selected value to your copy buffer which can then be pasted into your CSV file.
   - Click **Export Full Table**, in upper the right corner above the properties table, to save a copy of the properties table.
4. Locate the downloaded template and add your specific information to the template.
   - Users **AdminRoles** property: The value for the Authorizer Administrator is "GlobalAdmin".
   - Safeguard for Privileged Passwords does not add an object if any column contains invalid data in the .csv file with the follow exceptions:

NOTE: Safeguard for Privileged Passwords does not add an object if any column contains invalid data in the .csv file with the follow exceptions:

- Assets **PlatformDisplayName** property.
  1. If Safeguard for Privileged Passwords does not find an exact match, it looks for a partial match. If it finds a partial match it supplies the ***<platform>*** **Other** platform, such as "Other Linux".
  2. If it does not find a partial match, it supplies the **Other** platform type.
- Users **TimeZoneId** property.
  1. If Safeguard for Privileged Passwords does not find a valid TimeZoneId property (that is, does not find an exact match or no timezone was

provided), it uses the local workstation's current timezone. Do not enter numbers or abbreviations for TimeZoneId.

- Users **Password** property.
  1. Safeguard for Privileged Passwords adds a user without validating the password you provide.

5. Use the customized .csv file to import the objects.

Checking, changing, or setting an account password

The Asset Administrator can manually check, change, or set an account password from the **Account Security** menu.

To manually check, change, or set an account password

1. Navigate to **Administrative Tools** | **Accounts**.
2. In **Accounts**, select an account from the object list.
3. Click **Account Security** from the toolbar. You can also right-click the account name to open the context menu.

   Select one of these options:

   - **Check Password**to verify the account password is in sync with the Safeguard for Privileged Passwords database. If the password verification fails, you can change it.
   - **Change Password**to reset and synchronize the account password with the Safeguard for Privileged Passwords database.
   - **Set Password**to set the account password in the Safeguard for Privileged Passwords database. The Set option does not change the account password on the asset.

   NOTE: You can view the progress and results of the Check and Change options in the **Toolbox** | **Tasks** pane. For more information, see Viewing task status on page 145.

4. The **Set Password** option provides the following two options.
   a. **Generate Password**: Select this option to have Safeguard for Privileged Passwords generate a new random password, that complies with the password rule that is set in the account's profile.
      - Click **Generate Password** to display the **Generate Password** dialog.
      - Click **Show Password** to reveal the new password.
      - Click **Copy** to put it into your copy buffer.
      - log in to your device, using the old password, and change it to the password in your copy buffer.

- Click **OK** to change the password in the Safeguard for Privileged Passwords database or click **Cancel** to close the dialog without changing the current password in Safeguard for Privileged Passwords.

b. **Manual Password**: Select this option to manually set the account password in the Safeguard for Privileged Passwords database.

- Click **Manual Password** to display the **Set Password** dialog.
- In the **Set Password** dialog, enter and confirm the password. Click **OK** to update the Safeguard for Privileged Passwords database.
- Set the account password on the physical device to synchronize it with the Safeguard for Privileged Passwords 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 **Administrative Tools** | **Accounts**.
2. In **Accounts**, right-click an account name and choose **Password Archive**.

   Or, click **Password Archive** from the toolbar.
3. In the **Password Archive** dialog, select a date.

   TIP: 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.
4. In the **View** column, click to display the password that was assigned to the asset at that given date and time.
5. In the details dialog, click **Copy** to copy the password to your copy buffer, or click **OK** to close the dialog.

Account Groups

A Safeguard for Privileged Passwords 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 on page 276.

The Auditor and the Security Policy Administrator have permission to access **Account Groups**.

The **Account Groups** view displays the following information about the selected account group.

- General 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.

- **Add** | **Account Group**: Add account groups to Safeguard for Privileged Passwords. For more information, see Adding an account group on page 172.
- **Add** | **Dynamic Account Group**: Add dynamic account groups to Safeguard for Privileged Passwords. For more information, see Adding a dynamic account group on page 172.
- **Delete Selected**: Remove the selected account group from Safeguard for Privileged Passwords. For more information, see Deleting an account group on page 177.
- **Refresh**: Update the list of account groups.

  Add | **Account Group**: Add account groups to Safeguard for Privileged Passwords. For more information, see Adding an account group on page 172.

General tab (account group)

The **General** tab lists information about the selected Account Group.

Large tiles at the top of the tab display the number of **Accounts** and **Access Request Policies** associated with the selected account group.

Table 26: Account Groups General tab: General properties

Property	Description
Name	The selected account group's name
Account Rules	For dynamic account groups, a summary of the asset account rules defined
Description	Information about the selected account group

Related Topics

Modifying an account group

Accounts tab (account group)

The **Accounts** tab displays the accounts associated with the selected account group.

Click **+ Add Account** from the details toolbar to add one or more accounts to the selected account group.

Search: For more information, see Search box on page 111.

Table 27: 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	For directory accounts, the name of the domain the account is associated with.
Ignored	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.

Property	Description
Session Request	A check in this column indicates that session access requests are enabled for this account.
Needs a Password	Displays ⚠ if a password is not set for the selected account. For more information, see Checking, changing, or setting an account password on page 165.
Description	Information about the account.

Use these buttons on the details toolbar.

Table 28: Account Groups: Access Request Policies tab toolbar

Option	Description
+ **Add Account**	To add one or more accounts to the account group you selected.
— **Remove Selected**	Remove the selected account.
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 111.

Related Topics

Adding one or more accounts to an account group

Modifying an account group

Access Request Policies tab (account group)

The **Access Request Policies** tab displays the entitlements and policies, including password release and session request policies, associated with the selected account group.

Table 29: Account Groups: Access Request Policies tab properties

Property	Description
Entitlement	The name of the access request policy's entitlement
Access Request	The name of the policy that governs the accounts in the selected

Property	Description
Policy	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 30: Account Groups: Access Request Policies tab toolbar

Option	Description
Add to Policy	Add the selected account group to the scope of one or more access request policy. Clicking this button displays the **Access Request Policy** selection dialog, allowing you to select a policy.
Remove Selected	Remove the selected account group from the scope of the selected access policy.
Refresh	Update the list of access request policies.
Details	View and edit details about the selected access request policy. For more information, see Creating an access request policy.
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 111.

Related Topics

Adding accounts to an access request policy

Modifying an account group

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.

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.

- **Search**: For more information, see Search box on page 111.
- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Table 31: 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 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

Display event details

Select an event to display this additional information for some types of events (for example, create and update events).

Table 32: Additional History tab properties

Property	Description
Property	The property that was updated

Property	Description
Old Value	The value of the property before it was updated
New Value	The new value of the property

Managing account groups

Use the controls and tabbed pages in the Account Groups view to perform the following tasks to manage Safeguard for Privileged Passwords 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
- Modifying an account group
- Deleting an account group

Adding an account group

It is the responsibility of the Security Policy Administrator to add account groups to Safeguard for Privileged Passwords.

To add an account group

1. Navigate to **Administrative Tools** | **Account Groups**.
2. Click **+ Add** | **Account Group** from the toolbar.
3. In the **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 **Add Account Group**.

Adding a dynamic account group

It is the responsibility of the Security Policy Administrator to add dynamic account groups to Safeguard for Privileged Passwords.

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 **Administrative Tools** | **Account Groups**.
2. Click **+ Add** | **Add Dynamic Account Group** from the toolbar.
3. In the **Dynamic Account Group** dialog, provide information in each of the tabs:

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
Summary tab (add dynamic account group)	Where you review the rules defined for adding accounts to a dynamic account group, and where you save your selections, and add the 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 33: Dynamic Account Group: General tab

Property	Description
Name	Enter a unique name for the dynamic account group. Limit: 50 characters
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 34: 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** • **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

Property	Description
	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** • **Not equal** For boolean attributes (such as Service Account), 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. 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.
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.

Property	Description
	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.

Summary tab (add dynamic account group)

On the **Summary** tab of the **Dynamic Account Group** dialog, review the rules defined and add the dynamic account group.

1. Review the rules defined for this dynamic account group.
2. Return to the **Account Rules** tab to modify any of the rules if necessary.
3. Click **Add Account Group** to create the dynamic account 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 **Administrative Tools** | **Account Groups**.
2. Select an account group from the object list and click the **Accounts** tab.
3. Click **+ Add Account** from the details toolbar.
4. Select one or more accounts from the list in the **Accounts** selection dialog and click **OK**.

Create an account to add to an account group

If you do not see the account you are looking for and you have Asset Administrator permissions, you can click **+ Create New**. For more information the information to provide, see Adding an account. Click **OK** in the Accounts selection dialog to add the accounts to the selected account group.

Related Topics

Adding an account to one or more account groups

Adding accounts to an access request policy

To add accounts to an access request policy

1. Navigate to **Administrative Tools** | **Account Groups**.
2. In **Account Groups**, select an account group from the object list and open the **Access Request Policies** tab.
3. Click **+ Add to Policy** from the details toolbar.
4. Select a policy from the list in the **Access Request Policy** selection dialog and click **OK**.

Modifying an account group

To modify an account group's information

1. Navigate to **Administrative Tools** | **Account Groups**.
2. In **Account Groups**, select an account group from the object list.
3. Select the view of the account group's information you want to modify (**General**, **Accounts**, or **Access Request Policies**).

   For example:

   - To change the selected account group's name or description, click the **General** tab then click the **Edit** icon. You can also double-click an account group name to open the **General** settings edit window.
   - To add (or remove) accounts associated with the selected account group, click the **Accounts** tab. You can multi-select members to add or remove more than one from an account group.
   - To add (or remove) accounts in a dynamic account group, double-click the dynamic account group and change the selections on the **Account Rules** tab.
   - To add (or remove) the selected account group to the scope of a policy, switch to the **Access Request Policies** tab. For more information, see Access Request Policies tab (account group) on page 169.
4. To view or export the details of each operation that has affected the selected account group, switch to the **History** tab. To export, select the time frame then click **Export**.

Deleting an account group

When you delete an account group, Safeguard for Privileged Passwords does not delete the associated accounts.

To delete an account group

1. Navigate to **Administrative Tools** | **Account Groups**.
2. In **Account Groups**, select an account group.
3. Click 🗑 **Delete Selected**.
4. Confirm your request.

15

Assets

A Safeguard for Privileged Passwords asset is a computer, server, network device, or application managed by a Safeguard for Privileged Passwords Appliance.

It is the responsibility of the Asset Administrator to add assets and accounts to Safeguard for Privileged Passwords.The Auditor has permission to access **Assets**.

Before adding assets to Safeguard for Privileged Passwords, you must ensure they are properly configured. For more information, see Preparing systems for management on page 519.

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 identified on the General tab (asset group). All new assets are automatically governed by the default profile unless otherwise specified.

An asset can only be in one partition at a time identified on the General tab (asset group). 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 partition profile so that when you add assets, the assets are added to the default partition and default partition profile. For more information, see Setting a default partition on page 304.

Asset Discovery jobs run automatically against the directories you have added. For information about configuring asset discovery in Safeguard for Privileged Passwords, see Asset Discovery job workflow.

Assets view

The **Assets** view displays the following information about the selected system. Not all selections will be available for all assets.

- General tab (asset): Displays general, management and connection settings for the selected 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.

- Access Request Policies tab (asset): Displays the entitlements and access request policies associated with the selected asset.
- Asset Groups tab (asset): Displays the asset groups that contain the selected asset.
- Discovered Services tab (asset): Displays the details of each discovered service associated with the selected asset.
- History tab (asset): Displays the details of each operation that has affected the selected asset.

Toolbar

Use these toolbar buttons to manage assets:

- **Add Asset**: Add assets to Safeguard for Privileged Passwords. For more information, see Adding an asset on page 193.
- **Delete Selected**: Remove the selected asset. For more information, see Deleting an asset on page 219.
- IMPORTANT: When you delete an asset, you also permanently delete all the Safeguard for Privileged Passwords accounts associated with the asset.
- **Refresh**: Update the list of assets.
- **Import Assets**: Add assets to Safeguard for Privileged Passwords. For more information, see Importing objects on page 462.
- **Download SSH Key**: Add the SSH key to the selected asset. For more information, see Downloading a public SSH key on page 222.
- **Access Requests**: Allows you to enable or disable access request services for the selected asset. Menu options include **Enable Session Request** and **Disable Session Request**.
- **Syncronize Now**: Run the directory addition and deletion synchronization process on demand.
- **Show Disabled**: Display the assets that are not managed and are disabled and have no associated accounts. Asset management can be controlled by right-clicking on 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 right-clicking an asset and selecting **Enable-Disable**.

  Add Asset: Add assets to Safeguard for Privileged Passwords. For more information, see Adding an asset on page 193.

Asset menu options

Right click on an asset to use these context menu options.

- **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 (either via a discovery or import), certain tasks will not be available for accounts associated with the asset, such as Check System, Check Password, and Change Password.
- **Check Connection**: Select to verify that Safeguard for Privileged Passwords can log in to the asset using the current service account credentials. For more information, see Checking an asset's connectivity on page 212.
- **Syncronize Now**: Run the directory addition and deletion synchronization process on demand. In addition, it runs through the discovery, if there are discovery rules and configurations set up.
- **Download SSH Key**: Add the SSH key to the selected asset. For more information, see Downloading a public SSH key on page 222.
- **Enable-Disable**: Select **Enable** to have Safeguard for Privileged Passwords manage a disabled asset. This option is only available for assets that have been disabled. 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 Safeguard for Privileged Passwords from managing the selected asset. When you disable an asset, Safeguard for Privileged Passwords disables it and removes all associated accounts. If you choose to manage the asset later, Safeguard for Privileged Passwords re-enables all the associated accounts.
- **Access Requests**: Select **Enable Session Request** to allow session requests for the selected asset. Select **Disable Session Request** to disallow session requests for the selected asset.
- **Discovery Accounts**: Run the associated Account Discovery job. For more information, see Account Discovery on page 248.
- **Discover Services**: Run the associated Account Discovery job that has **Discovery Services** selected. For more information, see Adding an Account Discovery job on page 251.
- **Delete Selected**: Remove the selected asset from Safeguard for Privileged Passwords. When you delete an asset, you also permanently delete all the Safeguard for Privileged Passwords accounts associated with the asset.

General tab (asset)

The **General** tab lists information about the selected asset.

Large tiles at the top of the tab display the number of **Accounts**, **Account Dependencies** (when applicable), **Access Request Policies**, and **Asset Groups** associated with the selected asset. Clicking a tile heading opens the corresponding tab.

Navigate to **Administrative Tools** | **Assets** | **General**. The following fields display based on the type of asset (for example, Windows, Linux, OpenLDAP, or Active Directory).

Table 35: General tab: General properties

Property	Description
Name	The asset name.
Description	Descriptive text to further identify the asset.
Partition	The name of the partition where the selected asset resides.
Profile	The name of the profile that manages the asset's accounts. NOTE: All assets must be governed by a profile. All new assets are automatically governed by the default profile unless otherwise specified.
License Type	If applicable (for example, for a Windows asset), indicates your license model, such as System or Desktop.
Last Successful Account Discovery	If applicable, the date and time of the last successful Account Discovery job.
Next Account Discovery	If applicable, the date and time of the next automated Account Discovery job as set in the **Account Discovery** job of the partition profile. (For more information, see Creating a profile on page 302.)
Directory (directory)	The name of the directory where the asset was discovered.
Domain Name (directory)	The name of the domain where the asset was discovered.
NetBios Name (directory)	The NetBios name of the asset that was discovered.
Distinguished Name (directory)	The distinguished name of the asset that was discovered.

The following fields display based on the type of asset (for example, Windows, Linux, OpenLDAP, or Active Directory).

Table 36: General tab: Management properties

Property	Description
Product	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.
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	The managed domains.
Available for discovery across all partitions	If **True**, this asset is read-access available for Asset Discovery jobs beyond partition boundaries.
Managed Network	The managed network that is assigned for work load balancing. For more information, see Managed networks on page 369.
Enable Session Request	The check box is selected if session access requests are enabled for the asset.
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 sever used for SSH session access requests.
Telnet Session Port	If connecting to TN3270 or TN5250, the port for connection.
Sync additions every [number]	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 failed, and last successful sync display. The intervals are directory specific.

Property	Description
minutes	
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 sync, last failed, and last successful sync display. The intervals are directory-specific.

Table 37: General tab: Account Discovery properties

Account Discovery	Account discovery identifier
Last Successful Account Discovery	The date and time of the last successful account 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

Table 38: Assets General tab properties: Connection properties

Property	Description
Authentication Type	How the console connects with the managed system. For more information, see Connection tab (add asset) on page 200.
Service Account Name	The account used by Safeguard for Privileged Passwords to securely manage accounts and passwords on the asset.
Service Account Domain Name	The domain used to manage accounts and passwords on the asset.
Service Account Distinguished Name	The distinguished name of the service account.
Connection Timeout	The session timeout period.
Privilege Elevation Command	Displays the elevation command (such as sudo) if it is populated on the **Connection** tab.
Port	The port used by SSH to log in to the managed system.
SSH Host Key Fingerprint	The fingerprint of the SSH key that Safeguard for Privileged Passwords uses to authenticate to the asset.
SSH Key Comment	Human-readable information about the SSH key.
SSH Host Key Fingerprint	The managed system's public host key fingerprint. When an asset requiring an SSH host key does not have one, **Check Password** will fail. For more information, see Connectivity failures on page 540.

Property	Description
CheckSystem (custom platform script)	True if the service account has access to the remote host. See the wiki Writing a custom platform script.
CheckPassword (custom platform script)	True if the given account user and password are valid on the remote host. See the wiki Writing a custom platform script.
ChangePassword (custom platform script)	True if the password for the given user on the remote host. See the wiki Writing a custom platform script.

Table 39: Assets General tab properties: Attributes properties (for example, for directories and LDAP)

Property	Description
User Attributes	User attributes include: Object Class User Name Password Description
Group Attributes	Group attributes include: Object Class Name Member
Computer Attributes	Computer attributes include: Object Class Name Network Address Operating System Operating System Version Description

Tags: Tag assignments for the selected asset. The tiles listed under in the **Tags** pane display 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 pane.

Description: Information about the selected asset.

Related Topics

Assigning an asset to a partition

Assigning a profile to an asset

Modifying an asset

Accounts tab (asset)

An asset's **Accounts** tab displays the accounts associated with this asset.

Click **+Add Account** from the details toolbar to associate an account with the selected asset.

Navigation: **Administrative Tools** | **Assets** | **Accounts**.

Table 40: Assets: Accounts tab properties

Property	Description
Name	Name of an account associated with the selected asset. NOTE: 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.
Profile	The name of the profile that manages the account.
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. NOTE: 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. NOTE: Click **Access Requests** from the details toolbar to enable or disable a user's ability to request access to the selected account.
Needs a Password	Displays ⚠ if a password is not set for the account. For more information, see Checking, changing, or setting an account password on page 165.

Property	Description
Description	Descriptive information entered when the account was added.
Global Access	A ✔ check in this column indicates that the asset is available for discovery across all partitions. For more information, see Available for discovery across all partitions on page 196.

Use these buttons on the details toolbar to manage your asset accounts.

Table 41: Assets: Accounts tab toolbar

Option	Description
Add Account	Add accounts to the selected asset. For more information, see Adding an account to an asset on page 215.
Delete Selected	Remove the selected account from the asset.
Refresh	Update the list of asset accounts.
Account Security	Menu options include **Check Password**, **Change Password**, and **Set Password**. For more information, see Checking, changing, or setting an account password on page 165.
Password Archive	Display the password history for the selected asset account. For more information, see Viewing password archive on page 166.
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 Password Request, Session Request, or both. Menu options include: • Enable Password Request • Disable Password Request • Enable Session Request • Disable Session Request 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 254.
Set Profile	Select a profile to manage the selected asset account.

Option	Description
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 111.

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 Safeguard for Privileged Passwords.

Click + **Add Account** from the details toolbar to associate account dependencies with the selected asset. For more information, see Adding account dependencies on page 216.

Navigate to **Administrative Tools** | **Assets** | **Account Dependencies**.

Table 42: 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

Access Request Policies tab (asset)

The **Access Request Policies** tab displays the entitlements and access request policies associated with the selected asset.

Navigate to **Administrative Tools** | **Assets** | **Access Request Policies**.

Table 43: 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 policy that governs the selected asset

Property	Description
Assets	The number of unique assets that are associated with the access request policy
# Asset Groups	The number of unique asset groups in the access request policy
Asset Groups	The names of the asset groups that associate the selected asset with the policy

Use these buttons on the details toolbar to manage your access request policies associated with the selected asset.

Table 44: Assets: Access Request Policies tab toolbar

Option	Description
Add to Policy	Add the selected asset to the scope of a session access request policy.
Remove Selected	Remove the selected policy. For more information, see Deleting an access request policy on page 288.
Refresh	Update the list of access request policies.
Details	View and edit details about the selected access request policy. For more information, see Creating an access request policy.
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 111.

Asset Groups tab (asset)

The **Asset Groups** tab displays the asset groups that contain the selected asset.

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 37.. This section lists SPP and SPS support by platform.

The Auditor and Security Policy Administrator have permission to access **Asset Groups**.

Click **+ Add Asset Groups** from the details toolbar to add the selected asset to one or more asset groups.

Navigate to **Administrative Tools** | **Assets** | **Asset Groups**.

Table 45: Assets: Asset Groups tab properties

Property	Description
Name	The asset group name.
Dynamic	A check mark in this column indicates that the group is a dynamic asset group.
Description	Information about the asset group.

Related Topics

Adding an asset to asset groups

Discovered Services tab (asset)

The **Discovered Services** tab displays information specific to the selected asset and is applicable only to Windows assets.

- For more information, see Discovered Services on page 262.
- For more information about the workflow, see Account and Service Discovery job workflow.

Navigate to **Administrative Tools** | **Assets** | **Discovered Services**.

Use these buttons to manage the discovered services.

Table 46: Discovered Services: Toolbar

Option	Description
Discover Services	Run the selected service discovery job.
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 111.

The following displays for each discovered service.

Table 47: 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

Property	Description
	Active Directory account.
System Name	The asset to which the account is associated.
Account Status	The status of the Safeguard account. If Safeguard manages the account, the value is **Managed**. If the account is disabled, the value is blank.
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 you select the following options. Select the **Automatically Manage Found Accounts** option on the account discovery job associated with the partition profile that is associated to the asset. For more information, see Adding an Account Discovery rule on page 254.
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.

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.
- **Search**: For more information, see Search box on page 111.
- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Navigate to **Administrative Tools** | **Assets** | **History**.

Table 48: 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

Select an event to display this additional information for some types of events (for example, create and update events).

Table 49: Additional History tab properties

Property	Description
Property	The property that was updated
Old Value	The value of the property before it was updated
New Value	The new value of the property

Managing assets

Use the controls and tabbed pages on the **Assets** page to perform the following tasks to manage Safeguard for Privileged Passwords 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 an asset to asset groups
- Modifying an asset
- Deleting an asset
- Importing objects
- Downloading a public SSH key

Adding an asset

It is the responsibility of the Asset Administrator to add assets and accounts to Safeguard for Privileged Passwords.

Safeguard for Privileged Passwords allows you to set up Asset Discovery jobs that run automatically. For more information, see Asset Discovery job workflow on page 236.

Before you add systems to Safeguard for Privileged Passwords, make sure they are properly configured. For more information, see Preparing systems for management on page 519.

> 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 **Administrative Tools** | **Assets**.
2. Click **+Add Asset** from the toolbar.
3. In the **Asset** dialog, provide information in each of the tabs:

General tab (add asset)	Where you add general information about the asset
Management tab (add asset)	Where you add the network address, operating system, and version information
Account Discovery tab (add asset)	Where you add the Account Discovery job

Connection tab (add asset)	Where you add the authentication type information or custom platform properties
Attributes tab (add asset)	Where you add attributes to directory assets

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 profile

General tab (add asset)

Use the General tab to specify general information about the asset, including 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 and new assets are automatically governed by the default profile unless otherwise specified.

Table 50: Asset: General properties

Property	Description
Name	Enter a unique display name for the asset. Limit: 100 characters Required
Description	(Optional) Enter information about this managed system. Limit: 255 characters
Partition	**Browse** to select a partition for this asset. You can set a specific partition as the default, see Setting a default partition.
Profile	**Browse** to select a profile to manage this asset's accounts. You must assign all assets to a profile. Safeguard for Privileged Passwords assigns all new assets to the default profile unless you specify another. You can set a specific profile as the default. For more information, see Setting a default partition profile on page 305. 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, Safeguard for Privileged Passwords does

Property	Description
	not activate the **Reset** button. If you do not explicitly assign an asset to a profile, it is always assigned to the current default profile.

Management tab (add asset)

Use the **Administrative Tools** | **Assets** | **Management** tab to add the network address, operating system or directory service, and version information for an asset.

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 260.

The settings for an asset are shown below.

Table 51: Asset: Management tab properties (for example, Windows, Linux, OpenLDAP, or Active Directory)

Property	Description
Product	Select an operating system or directory service, for this asset. A custom platform can be selected. For more information, see Custom platforms on page 333. NOTE: Safeguard for Privileged Passwords allows you to select a generic operating system of **Other**, **Other Managed**, or **Other Linux**. This allows you to add an asset to Safeguard for Privileged Passwords 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. Safeguard for Privileged Passwords cannot connect to the asset so there is no automatic password check and change, test connection, or other activity requiring a connection. • **Other Managed**: Safeguard for Privileged Passwords stores the password 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 make use of the password in configuration files. For example, a listener can pick up the change event via the Safeguard for Privileged Passwords Application to Application (A2A) service and perform actions, as required. • **Other Linux**: Safeguard for Privileged Passwords manages

Property	Description
	an asset with "Other Linux" on a best effort basis. **Other** platform details: Any **Other** platform type can be changed to 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 an **Other 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. For more information, see Modifying an asset on page 218.
Version	If applicable, select the operating system version. When adding a Linux or Macintosh OS X system, Safeguard for Privileged Passwords allows you to choose an **Other** version. NOTE: Safeguard for Privileged Passwords 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 information, see Adding an account to an asset on page 215.
Architecture	If applicable, the product's system architecture.
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.
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.
Manage Forest (directory)	Select if you want to manage the whole forest. Do not select if you want to manage just one domain.
Available for discovery across all partitions	If applicable, select to make this asset read-access available for Asset Discovery jobs beyond partition boundaries. Any partition that exists is able to use this directory asset. Other partition owners do not have read password access. If not selected, partition owners and other partitions will not know the directory asset exists. In setting up the Asset Discovery job, use the **Directory** asset discovery **Method** so that directory assets that are shared can be discovered into any partition. For more information, see General tab (asset discovery) on page 237.
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

Property	Description
	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.
Advanced	
Managed Network	The managed network that is assigned for work load balancing. For more information, see Managed networks on page 369.
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	For directory assets, enter or select how often you want Safeguard for Privileged Passwords 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. Default: 15 minutes Range: Between 1 and 2147483647 Directory Sync is enabled by default and can be disabled. For more information, see Enable or Disable Services (Access and management services) on page 309.
Sync deletions every [number] minutes	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 deletions that have been made to the objects, including group membership and user account attributes mapped to Safeguard for Privileged Passwords. Default: 15 minutes Range: Between 1 and 2147483647 Directory Sync is enabled by default and can be disabled. For more information, see Enable or Disable Services (Access and management services) on page 309.

Account Discovery tab (add asset)

The Account Discovery tab is only available after Active Directory Asset has been created. On the **Account Discovery** tab, the default is `Do not perform account discovery`.

Table 52: Account Discovery tab properties

Property	Description
Description	Select the description of the Account 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.
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.) • 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. • **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**

Property	Description
	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 **-** delete 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 AM** • **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 that 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 20:00:00 PM** and **Repeat 2**. • **Time Zone**: Select the time zone.
Rules	You may 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 inform-

Property	Description
	ation, see Adding an Account Discovery rule on page 254. • **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 Safeguard for Privileged Passwords. • **Set default password**: A check mark displays if the rule causes default passwords to be set automatically. • **Assign to Profile**: The partition profile assigned • **Assign to Sync Group**: A check mark displays if the rule automatically associated the accounts with a password 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.

Connection tab (add asset)

On the **Connection** tab, choose an **Authentication Type** (see the table that follows) and specify the service account credentials. The type of asset specified in the **Product** field on the **Management** tab determines the authentication types available for the asset. If the asset has a custom platform, the **Custom Properties** elements are displayed. For more information, see Custom platforms on page 333.

Table 53: 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 147.
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.

Authentication Type	Description
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 157.
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 157.
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 333.
None	No authentication information is taken and check/change 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 the connection timeout period.

Client ID: For SAP assets, enter the client ID.

Custom platform properties

If the **Product** field on the **Management** tab identified a custom platform, complete the dialog based on the custom properties of the custom platform script. Safeguard for Privileged Passwords 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). Safeguard for Privileged Passwords cannot check the validity or system impact of values entered for custom platforms. For more information, see Creating a custom platform script on page 334.

About service accounts

Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords adds its service account to the list of **Accounts** and designates it with a **Service Account** icon. By default, Safeguard for Privileged Passwords automatically manages the service account password according to

the check and change schedules in the profile that governs its asset. For more information, see Creating a profile on page 302.

When adding a service account, Safeguard for Privileged Passwords automatically disables it from access requests. If you want the password to be available for release, click **Access Requests** and select **Enable Password Request**. If you want to enable session access, select **Enable Session Request**.

> TIP: As a best practice, if you do not want Safeguard for Privileged Passwords to manage a service account password, add the account to a profile that is set to never change passwords.

If you delete a service account, Safeguard for Privileged Passwords changes the asset's authentication type to **None**, which disables automatic password management for all accounts that are associated with this asset. A user can continue to check out the passwords, however, if the policy that governs the account requires that it change the password after release, the password can get stuck in a pending password reset state. For more information, see Password is pending a reset on page 548.

Test connectivity

The most common causes of failure in Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords), 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords can log in to the asset using the service account credentials that you have provided.

Once you save the new asset, Safeguard for Privileged Passwords saves the service account credentials. Safeguard for Privileged Passwords 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 201.

If you want to verify an existing asset's connectivity, use the **Check Connection** right-click command. For more information, see Checking an asset's connectivity on page 212.

Related Topics

Test Connection failures

SSH Key

You can configure Safeguard for Privileged Passwords to authenticate to a managed system using an SSH authentication key. Safeguard for Privileged Passwords will not rotate SSH Keys unless you select the **Manage SSH Key** option in the asset's profile change schedule. For more information, see Adding change password settings on page 426.

> NOTE: This option is not available for all operating systems. But if a Safeguard for Privileged Passwords asset requires an SSH host key and does not have one, **Check Password**, **Change Password**, and **Test Connection** will fail. For more information, see Connectivity failures on page 540.

Table 54: SSH Key authentication type properties

Property	Description
Automatically Generate the SSH Key	Select this option to have Safeguard for Privileged Passwords generate the SSH authentication key.
Manually Deploy the SSH Key	When you select **Automatically Generate the SSH Key**, Safeguard for Privileged Passwords allows you to select this option so that you can manually append this public key to the authorized keys file on the managed system for the service account. For more information, see Downloading a public SSH key on page 222. The SSH authentication key becomes available after Safeguard for Privileged Passwords creates the asset. IMPORTANT: If you do not select this option, Safeguard for Privileged Passwords automatically installs the SSH authentication key. If you do select this option, Safeguard for Privileged Passwords creates the key and associates it with the Safeguard for Privileged Passwords asset you are creating, but it does not install it on the managed system for you.
Import and Manually Deploy the SSH Key	Select this option, then **Browse** to import an SSH authentication key. For more information, see Importing an SSH key on page 205.
Key Comment	(Optional) Enter a description of this SSH key.
Service Account Name	Enter the service account name that Safeguard for Privileged Passwords is to use for management tasks. This is the account Safeguard for Privileged Passwords uses to install the SSH authentication key on the asset. For more information, see About service accounts on page 201.
Service Account Password	If not importing the SSH authentication key, then you must enter the service account password Safeguard for Privileged Passwords needs to authenticate to this managed system. Limit: 255 characters

Property	Description
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 passwords and to discover accounts. When adding an asset, Safeguard for Privileged Passwords uses this command to perform **Test Connection**. For more information, see About Test Connection on page 202. To enable Safeguard for Privileged Passwords to elevate the privileges of the service account, assign the asset to the scope of a partition profile that has the privilege elevation command defined. For more information, see Creating a profile on page 302. 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 534. Limit: 255 characters
Test Connection	Click this button to verify that Safeguard for Privileged Passwords can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 202.
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 General tab (account) on page 148.
Auto Accept SSH Host Key	Select this option to have Safeguard for Privileged Passwords automatically accept the SSH host key when it creates the Safeguard for Privileged Passwords asset. When this option is selected, Safeguard for Privileged Passwords 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 Password** will fail. For more information, see Connectivity failures on page 540.
Port	Enter the port number used by SSH to log in to the managed system. Required
Connection Timeout	Enter the command timeout period. This option applies only to platforms that use telnet or SSH. Default: 20 seconds

Importing an SSH key

When you add an asset using the **SSH Key** authentication type, Safeguard for Privileged Passwords gives you the option to **Use an Imported SSH Key**.

To import an SSH Key

1. Click **+ Add Asset** from the toolbar to add an asset.
2. In the Connection tab:
   a. In **Authentication type**, select **SSH Key**.
   b. In **SSH Key Generation and Deployment Settings**, select **Import and Manually Deploy SSH Key**.
   c. **Browse** to select an SSH key.
3. In the **SSH Key** dialog, click **Import an SSH Key**.
4. In the **Import an SSH Key** dialog, specify the following information:
   a. In **Private Key File**, **Browse** to select a private key file.
   b. In **Key Comment**, enter a comment regarding the key.
   c. Click **Import**.

Directory Account

You can configure Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords and add domain user accounts. For more information, see Accounts on page 147.

Table 55: 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 Safeguard for Privileged Passwords.
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 passwords and to discover accounts. When adding an asset, Safeguard for Privileged Passwords

Property	Description
	uses this command to perform **Test Connection**. For more information, see About Test Connection on page 202. To enable Safeguard for Privileged Passwords to elevate the privileges of the service account, assign the asset to the scope of a partition profile that has the privilege elevation command defined. For more information, see Creating a profile on page 302. 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 534. Limit: 255 characters
Test Connection	Click this button to verify that Safeguard for Privileged Passwords can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 202.
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 General tab (account) on page 148.
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	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 Safeguard for Privileged Passwords 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 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

Property	Description
	certificate to the Trusted Certificates store. Only clear the **Verify SSL Certificate** option if you do not want to establish trust with the asset's
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 Safeguard for Privileged Passwords 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 540.
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.

Local System Account

You can configure Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords.

Table 56: Local System Account authentication type properties

Property	Description
Service Account	Click **Select Account** to choose the local system account associated with the SQL Server for Safeguard for Privileged Passwords to use for management tasks.
Test Connection	Click this button to verify that Safeguard for Privileged Passwords can log in to this asset using the local system account credentials you have provided. For more information, see About Test Connection on page 202.
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.

Property	Description
Advanced	Open to reveal the following settings:
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 Administrative Accounts and Privileges and SYSDBA and SYSOPER System Privileges.
Instance (Service Name)	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. Specify the Service Name if you are configuring an Oracle asset.
Port	Enter the port number to log in to the asset.
Connection Timeout	Enter the SQL server connection timeout period. Default: 20 seconds

Password (local service account)

You can configure Safeguard for Privileged Passwords to authenticate to a managed system using a local service account and password.

NOTE: Some options are not available for all operating systems.

Table 57: 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 Name	**Browse** to select the service account for Safeguard for Privileged Passwords to use for management tasks. When you add the asset, Safeguard for Privileged Passwords automatically adds the service account to **Accounts**. For more information, see About service accounts on page 201. Required except for LDAP platforms, which use the Distinguished Name.
Service Account Password	Enter the service account password used to authenticate to this asset.

Property	Description
	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 passwords and to discover accounts. When adding an asset, Safeguard for Privileged Passwords uses this command to perform **Test Connection**. For more information, see About Test Connection on page 202. To enable Safeguard for Privileged Passwords to elevate the privileges of the service account, assign the asset to the scope of a partition profile that has the privilege elevation command defined. For more information, see Creating a profile on page 302. 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 534. Limit: 255 characters
Privilege Level Password	Enter the Enable password to allow access to the Cisco configuration.
Test Connection	Click this button to verify that Safeguard for Privileged Passwords can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 202.
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 General tab (account) on page 148.
Auto Accept SSH Host Key	This check box is selected by default indicating that Safeguard for Privileged Passwords automatically accepts an SSH host key. This option is not available for all platforms. 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 540.
Use SSL Encryption	Select this option to enable Safeguard to encrypt

Property	Description
	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 Safeguard for Privileged Passwords 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 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 Certificates store. Only clear the **Verify SSL Certificate** option if you do not want to establish trust with the asset's
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 Administrative Accounts and Privileges and SYSDBA and SYSOPER System Privileges.
Instance (Service Name)	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. Specify the Service Name if you are configuring an Oracle asset.
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 the connection timeout period. Default: 20 seconds

Access Key

You can configure Safeguard for Privileged Passwords to authenticate to a managed system using an access key.

Table 58: Access Key authentication type properties

Property	Description
Service Account	Enter an account for Safeguard for Privileged Passwords to use for management tasks. For more information, see About service accounts on page 201.
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.
Test Connection	Click this button to verify that Safeguard for Privileged Passwords can log in to this asset using the service account credentials you have provided. For more information, see About Test Connection on page 202.
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**, Safeguard for Privileged Passwords 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 it.

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.

Attributes tab (add asset)

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 59: Active Directory and LDAP: Attributes tab

Safeguard for Privileged Passwords Attribute	Directory Attribute
Users	
Object Class	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.
User Name	`sAMAccountName` for Active Directory, `cn` for LDAP
Password	`userPassword` for LDAP
Description	`description`
Groups	
Object Class	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 Attributes	
Object Class	Default: `computer` for Active Directory, `ipHost` for LDAP Cllick **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
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 Safeguard for Privileged Passwords can log in to it using the **Check 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 Safeguard for Privileged Passwords it saves these credentials.

The **Check 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 **Administrative Tools** | **Assets**.
2. From **Assets**, right-click an asset in the object list to open the asset's context menu.
3. Choose the **Check Connection** option.

   Safeguard for Privileged Passwords displays a Toolbox task pane that shows the results.

Related Topics

About Test Connection

About service accounts

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 **General** properties.

To assign an asset to a partition

1. Navigate to **Administrative Tools** | **Assets**.
2. In **Assets**, double-click an asset to open the general properties, or click the ✎ **Edit** icon next to the **General** title on the **General** tab.
3. On the **Asset** dialog, **Browse** to select a partition.
4. Click **OK**.

Related Topics

Adding assets to a partition

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 **Administrative Tools** | **Assets**.
2. In **Assets**, double-click an asset to open the general properties, or click the ✎ **Edit** icon next to the **General** title on the **General** tab.
3. **Browse** to select a profile, and click **OK**. You can only choose profiles that are in the selected asset's partition.
4. Click **Reset** to set the profile to the current default.

Related Topics

Assigning assets or accounts to a profile

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 341.

To manually add a tag to an asset

1. Navigate to **Administrative Tools** | **Assets**.
2. Select an asset from the object list (left-pane).
3. Open the **General** tab and scroll down to view the **Tags** pane.
4. Click ✎ next to the **Tags** title.
5. Place your cursor in the edit box and enter the tag to be assigned to the selected asset.

   As you type, existing tags that start with the letters entered will appear, allowing you to select a tag from the list.

   To add additional tags, press **Enter** before entering the next tag.
6. Click **OK**.

   If you do not see the new tag, click ↻ **Refresh**.
7. To remove a manually assigned tag, click the **X** inside the tag box.

Adding an account to an asset

Use the **Accounts** tab on the **Assets** view to add an account to an asset. You can acc 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 **Administrative Tools** | **Assets**.
2. In **Assets**, select an asset from the object list and open the **Accounts** tab.
3. Click **+Add Account** from the details toolbar.
4. Enter the account information and click **Add Account**.
5. In the **Account** dialog, 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.
   - **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 profile on page 305.
   - **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 he or she is an authorized user.
   - (For directory accounts only) **Available for use across all partitions**: 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.

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 **Administrative Tools** | **Assets**.
2. In **Assets**, select a directory asset from the object list and open the **Accounts** tab.
3. Click **+Add Account** from the details toolbar.
4. In the **Find Accounts** dialog, click **Browse** to select a container within the directory as the **Filter Search Location**.
   a. 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.
   b. In the **Name** field, enter a full or partial account name and click **Search**.

      To search for a directory account, you must enter text into the search box. Safeguard for Privileged Passwords searches each domain of a forest. You can search on partial strings. For example, if you enter "ad," it will find any user **Name** or **Distinguished Name** that contains "ad." The text search is not case-sensitive and does not allow wild cards.
5. The results of the search displays in the **Select the Account(s) to Add** grid. Select one or more accounts to add to Safeguard for Privileged Passwords.

Related Topics

Adding account dependencies

Setting a default partition profile

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.

Safeguard for Privileged Passwords performs dependent system updates to maintain the passwords for dependent accounts on all the systems that use them. For example, when Safeguard for Privileged Passwords 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.

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 156.
   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 156.
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. The service account must be a domain account if the asset is Windows SSH platform, but does not have to be a domain account if the asset is a Windows Server platform.
   Follow these steps:
   a. Navigate to **Administrative Tools** | **Assets**.
   b. Select a the asset (such as a Windows server) from the object list and open the **Account Dependencies** tab.
   c. Click + **Add Account** from the details toolbar and select one or more directory accounts. Safeguard for Privileged Passwords only allows you to select directory accounts.
3. Discovery: To update the asset, you must configure the Account Discovery job for the dependent asset. Navigate to **Administrative Tools** | **Discovery** | **Account Discovery** and select these check boxes:
   - **Discover Services**
   - **Automatically Configure Dependent System**.

   For more information, see Adding an Account Discovery job on page 251.
4. Partition profiles:
   a. The target directory account must be in the same partition profile as the dependent asset.
   b. You must configure the dependent asset's partition 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 profile on page 302.

Adding an asset to asset groups

Use the **Asset Groups** tab on the **Assets** view to add an asset to one or more asset groups.

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 37.. This section lists SPP and SPS support by platform.

To add an asset to asset groups

1. Navigate to **Administrative Tools** | **Assets**.
2. In **Assets**, select an asset from the object list and open the **Asset Groups** tab.
3. Click **+ Add Asset Group** from the details toolbar.
4. Select one or more asset groups from the list in the **Asset Groups** selection dialog and click **OK**.

If you do not see the asset group you are looking for and have Security Policy Administrator permissions, you can click **+ Create New** and add the new asset group. Enter the information and click **Add Asset Group**. For more information on creating asset groups, see Adding an asset group.

Modifying an asset

You can modify an asset.

To modify an asset

1. Navigate to **Administrative Tools** | **Assets**.
2. In **Assets**, select an asset from the object list.
3. Select the view of the asset's information you want to modify (such as **General**, **Accounts**, or **Account Dependencies**, **Access Request Policies**, **Asset Groups**, **Discovered Services**, or **History**).

   For example:

   - To change an asset's connection information, for example, connection timeout, double-click the **Connection** information in the **General** tab or click the ✎ **Edit** icon. You can also double-click an asset name to open the **General** settings edit window.

     NOTES:

     The following notes apply to attempting to change information on the **General** tab.

- **Profile**: You can only edit or remove a Service Account Profile when adding an asset. To update or remove the asset's service account profile, go to **Accounts**, select the service account, and edit it to update the profile. For more information, see General tab (account) on page 148.
- **Management** tab, **Product**: **Other** platform details: Any **Other** platform type can be changed to 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 an **Other 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.

- To add (or remove) an account to this asset, switch to the **Accounts** tab.
- To add (or remove) a directory account to a Windows server as an account dependency, switch to the **Account Dependencies** tab. For more information, see Adding account dependencies on page 216.

4. To view or export the details of each operation that has affected the selected asset, switch to the **History** tab. To export, select the time frame then click **Export**.

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 Safeguard for Privileged Passwords accounts associated with the asset.

To delete an asset

1. Navigate to **Administrative Tools** | **Assets**.
2. In **Assets**, select an asset from the object list.
3. Click **Delete Selected**.
4. Confirm your request.

Importing objects

Safeguard for Privileged Passwords 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. For more information, see Creating an import file on page 164.

Once an import is completed, you can navigate to the **Tasks** pane in the Toolbox for details about the import process and invalid data messages. For more information, see Viewing task status on page 145.

To import objects

1. In **Administrative Tools**, click **Assets**, **Accounts**, or **Users** based on what data you are importing.
2. Click **Import** from the toolbar.
3. In the **Import** dialog, **Browse** to select an existing .csv file containing a list of objects to import.
4. When importing assets, the **Discover SSH Host Keys** option is selected by default indicating that Safeguard will retrieve the required SSH host key for the assets specified in the .csv file.
5. Click **OK**.

   Safeguard for Privileged Passwords imports the objects into its database.

   NOTE: Safeguard for Privileged Passwords does not add an object if any column contains invalid data in the .csv file, with the following exceptions:

   - Assets **PlatformDisplayName** property:
     1. If Safeguard for Privileged Passwords does not find an exact match, it looks for a partial match. If it finds a partial match, it supplies the ***<platform>*** **Other** platform, such as **Other Linux**.
     2. If it does not find a partial match, it supplies the **Other** platform type.
   - Users **TimeZoneId** property:
     1. If Safeguard for Privileged Passwords does not find a valid TimeZoneId property (that is, does not find an exact match or no time zone was provided), it uses the local workstation's current time zone.

        NOTE: Do not enter numbers or abbreviations for the TimeZoneId.
   - Users **Password** property:
     1. Safeguard for Privileged Passwords adds a user without validating the password you provide.

Details for importing directory assets, service accounts, users, and user groups

You can use the steps like those above to import your existing directory infrastructure (such as Microsoft Active Directory). Managed account users cannot be members of the Protected Users AD Security Group.

Additional information specific to directory import follows.

1. Import the directory (and service account) via **Administrative Tools** | **Assets** | **Import Asset** and browse to select the .csv file. Safeguard for Privileged Passwords imports the directory as an asset.

   The directory's service account is automatically added to the list of accounts you can viewed via the **Assets** | **Accounts** tab.

   - By default, the service account password is automatically managed according to the check and change settings in the profile that governs the partition. For

more information, see Creating a profile on page 302. If you do not want Safeguard for Privileged Passwords to manage the service account password, assign the account to a profile that is set to never change passwords. For more information, see Assigning assets or accounts to a profile on page 305.

- The service account is added to the asset's Accounts tab and is disabled for password request and session request. For more information, see Accounts tab (asset) on page 186.
- To change either setting, navigate to **Administrative Tools** | **Accounts** and double-click the account. Then select the following check boxes, as desired: **Enable Password Request** and **Enable Session Request**. For more information, see General tab (account) on page 148.

2. Import users and user groups.

   a. Import directory users via **Administrative Tools** | **Users** | **Import Users** and browse to select the .csv file.

   b. Assign to user groups via **Administrative Tools** | **Users Groups** | **Users** (select one or multiple users).

   c. Automatic synchronization: Once you import directory users and directory groups, Safeguard for Privileged Passwords automatically synchronizes the objects in its database with the directory schema attributes. User and group membership changes in the directory are reflected in Safeguard for Privileged Passwords. Directory users authenticate to Safeguard for Privileged Passwords with their directory credentials.

Active Directory and LDAP synchronization

Active Directory and LDAP data is automatically synchronized by asset or identity and authentication providers schema as shown in the following lists.

Asset schema list

- Users
  - Username
  - Password (modifiable in LDAP and not modifiable in Active Directory)
  - Description
- Groups
  - Name
  - Member
- Computer
  - Name
  - Network Address
  - Operating System
  - Operating System Version
  - Description

Identity and Authentication Providers schema list

- Users
    - Username
    - First Name
    - Last Name
    - Work Phone
    - Mobile Phone
    - Email
    - Description
    - External Federation Authentication
    - Radius Authentication
    - Managed Objects
- Groups
    - Name
    - Members
    - Description

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), Safeguard for Privileged Passwords 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 **Administrative Tools** | **Assets**.
2. In **Assets**, select an asset that has an SSH key authentication type.
3. Click the **Download SSH Key** from the toolbar or the context menu.

   -OR-

   Open the asset's **Connection** settings and select **Download SSH Key**.
4. In the **Save As** dialog, specify the drive, directory, and name of the file to save.

You can manually install this public key to an asset.

16

Asset Groups

A Safeguard for Privileged Passwords 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 on page 276.

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 37.. This section lists SPP and SPS support by platform.

The Auditor and the Security Policy Administrator have permission to access **Asset Groups**.

The **Asset Groups** view displays the following information about the selected asset group.

- General tab (asset group): Displays general information about the selected asset group.
- Assets tab (asset group): Displays the assets associated with the selected asset group.
- Access Request Policies tab (account 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.

- **Add** | **Asset Group**: Add asset groups to Safeguard for Privileged Passwords. For more information, see Adding an asset group on page 227.
- **Add** | **Dynamic Asset Group**: Add dynamic asset groups to Safeguard for Privileged Passwords. For more information, see Adding a dynamic asset group on page 228.
- **Delete Selected**: Remove the selected asset group from Safeguard for Privileged Passwords. For more information, see Deleting an asset group on page 232.
- **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 111.

General tab (asset group)

The **General** tab lists information about the selected asset group.

The large tile at the top of the tab displays the number of **Assets** and **Access Request Policies** associated with the selected asset group. Clicking a tile heading opens the corresponding tab.

Table 60: Asset Groups General tab: General properties

Property	Description
Name	The selected asset group's name
Description	Information about the selected asset group
Asset Rules	For dynamic asset groups, a summary of the asset rules defined.

Related Topics

Modifying an asset group

Assets tab (asset group)

The **Assets** tab displays the assets associated with the selected asset group.

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 111.

Table 61: Asset Groups: Assets tab properties

Property	Description
Name	The asset name assigned to the managed system.
Platform Type	The platform of the managed system.
Session Request	A check in this column indicates that session access requests are enabled for the asset.
Description	Information about the asset.

Related Topics

Adding assets to an asset group

Modifying an asset group

Access Request Policies tab (asset group)

The **Access Request Policies** tab displays the entitlements and access request policies associated with the selected asset group.

Click **+ Add to Policy** from the details toolbar to add the selected asset group to the scope of one or more access request policies.

Table 62: 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 63: Asset Groups: Access Request Policies tab toolbar

Option	Description
+ Add to Policy	Add the selected asset group to the scope of an access request policy.
— Remove Selected	Remove the selected policy. For more information, see Deleting an access request policy on page 288.
Refresh	Update the list of access request policies.
Details	View and edit details about the selected access request policy. For more information, see Creating an access request policy on page 276.

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 111.

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.

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.
- **Search**: For more information, see Search box on page 111.
- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Table 64: 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 NOTE: A membership operation indicates a "relationship" change with a related or parent object such as the selected asset group

Property	Description
	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

Select an event to display this additional information for some types of events (for example, create and update events).

Table 65: Additional History tab properties

Property	Description
Property	The property that was updated
Old Value	The value of the property before it was updated
New Value	The new value of the property

Managing asset groups

Use the controls and tabbed pages in the Asset Groups view to perform the following tasks to manage Safeguard for Privileged Passwords asset groups:

- Adding an asset group
- Adding a dynamic asset group
- Adding assets to an asset group
- Modifying 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 Safeguard for Privileged Passwords.

Use the **Asset Groups** view to add new asset groups to Safeguard for Privileged Passwords.

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 37.. This section lists SPP and SPS support by platform.

To add an asset group

1. Navigate to **Administrative Tools** | **Asset Groups**.
2. Click **+ Add Asset Group** from the toolbar.
3. In the **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
4. Click **Add Asset Group**.

Adding a dynamic asset group

It is the responsibility of the Security Policy Administrator to add asset groups to Safeguard for Privileged Passwords.

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 37.. This section lists SPP and SPS support by platform.

To add a dynamic asset group

1. Navigate to **Administrative Tools** | **Asset Groups**.
2. From **Asset Groups**, click **+ Add** | **Add Dynamic Asset Group** from the toolbar.
3. In the **Dynamic Asset Group** dialog, provide information in each of the tabs.

General tab (add dynamic account group)	Where you add general information about the dynamic asset group
Account Rules tab (add dynamic account group)	Where you define the rules to be used to identify what assets are to be included in the dynamic asset group
Summary tab (add dynamic account group)	Where you review the rules defined for adding assets to this dynamic asset group, and where you save your selections and create 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 **Dynamic Asset Group** dialog, supply general information about the dynamic asset group.

Table 66: 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 **Dynamic Asset Group** dialog to define what assets are to be included in the dynamic asset group.

Table 67: 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**

Property	Description
	• **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.) • **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

Property	Description
	search criteria.
Preview	Click **Preview** to run the query in order to review the results of the query before adding the dynamic group.

Summary tab (add dynamic asset group)

On the **Summary** tab of the **Dynamic Asset Group** dialog, review the rules defined for adding assets to the dynamic asset group, save your selections, and add the dynamic asset group to Safeguard for Privileged Passwords.

1. Review the rules defined for this dynamic asset group.
2. Return to the **Asset Rules** tab to modify any of the rules if necessary.
3. Click **Add Asset Group** to create the dynamic asset 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 **Administrative Tools** | **Assets Groups**.
2. In **Asset Groups**, select an asset group from the object list and open the **Assets** tab.
3. Click **+ Add Asset** from the details toolbar.
4. Select one or more assets from the list in the **Assets** selection dialog and click **OK**.

   | NOTE: You can also double-click an asset name to add it.

If you do not see the asset you are looking for, depending on your Administrator permissions, you can create it in the Assets selection dialog. (You must have Asset Administrator permissions to create assets.)

To create a new asset from the Assets selection dialog

1. Click **+Create New**.

   For more information on creating assets, see Adding an asset.
2. Create additional assets, as required.
3. Click **OK** in the Assets selection dialog to add the assets to the selected asset group.

Modifying an asset group

To modify an asset group's information

1. Navigate to **Administrative Tools** | **Asset Groups**.
2. In **Asset Groups**, select an asset group from the object list.
3. Select the view of the asset group's information you want to modify (**General** or **Assets**).

   For example:

   - To change an asset group's name or description, double-click the **General** information in the **General** tab or click the ✎ **Edit** icon. You can also double-click an asset group name to open the **General** settings edit window.
   - To add (or remove) assets to the selected asset group, open the **Assets** tab.
4. To view or export the details of each operation that has affected the selected asset group, open the **History** tab.

Deleting an asset group

You can delete an asset group. When you delete an asset group, Safeguard for Privileged Passwords does not delete the associated assets.

To delete an asset group

1. Navigate to **Administrative Tools** | **Asset Groups**.
2. In **Asset Groups**, select an asset group from the object list.
3. Click 🗑 **Delete Selected**.
4. Confirm your request.

17

Discovery

Safeguard for Privileged Passwords discovery jobs can find assets, accounts, 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 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 asset discovery **Method** of **Directory**, 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 partition 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 156.

- **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.

Discovery tiles include the following:

- Asset Discovery: The number of Asset Discovery jobs available to run against the directories or networks to discover assets for potential management displays. Click the tile for detail.
- Asset Discovery Results: The number of Asset Discovery Results in the time frame indicated displays. Click the tile for detail.
- Account Discovery: The number of Account Discovery jobs available to run against the in scope assets to discover accounts for potential management displays. Click the tile for detail.
- Account Discovery Results: The number of Account Discovery Results in the time frame indicated displays. Click the tile for detail.
- Discovered Accounts: The number of discovered accounts in the specified partition displays. Click the tile for detail.
- Discovered Services: The number of discovered services in the specified partition displays. Click the tile for detail. You can launch discover service account jobs from **Administrative Tools** | **Assets** | **Discovered Services**. For more information, see Discovered Services tab (asset) on page 190.

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 Safeguard for Privileged Passwords. 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 on page 193.

If you use asset discovery **Method** of **Directory**, 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 Network Scan or Directory method of asset discovery, the **Other Linux** operating system is applied which you can modify later. For more information, see Modifying an asset on page 218.

For more information, see Asset Discovery job workflow on page 236.

Properties and toolbar

Navigate to **Administrative Tools** | **Discovery** | **Asset Discovery**.

Use these toolbar buttons to manage the discovery job settings.

Table 68: Asset Discovery: Toolbar

Option	Description
Add	Add an Asset Discovery job. For more information, see Adding an Asset Discovery job on page 236.
Delete Selected	Delete the selected Asset Discovery job.
Refresh	Update the list of Asset Discovery jobs that have run.
Edit	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.
Details	View additional details about the selected Asset Discovery job including schedule frequency and rules.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 111.

Asset Discovery jobs display in the grid.

Table 69: Asset Discovery: Asset Discovery job grid

Name	Name of the discovery job
Creator	Indicates how the job was launched, for example, Automated System or Admin
Method	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.

1. Create an Asset Discovery job. For more information, see Adding an Asset Discovery job on page 236.
2. After you save the Asset Discovery job, you can test it by selecting **Run Now**. For more information, see Asset Discovery on page 234.
3. After the Asset Discovery job runs, click the **Asset Discovery Results** tile to view the assets found. For more information, see Asset Discovery Results on page 247.
4. To control management of an asset, navigate to **Administrative Tools** | **Assets**, right-click the asset, click **Enable-Disable**, and choose one of these context menu options.

Enable	Select **Enable** to have Safeguard for Privileged Passwords manage a disabled asset. This option is only available for assets that have been disabled.
Disable	Select **Disable** to prevent Safeguard for Privileged Passwords from managing the selected asset. When you disable an asset, Safeguard for Privileged Passwords disables it and removes all associated accounts. If you choose to manage the asset later, Safeguard for Privileged Passwords re-enables all the associated accounts.

5. On **Administrative Tools** | **Assets**, you can show or hide assets marked as disabled, use the following buttons. For more information, see Assets on page 179.

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. Safeguard for Privileged Passwords lists the Asset Discovery events in the **Asset Discovery Activity** category.

Adding an Asset Discovery job

You can add a new Asset Discovery job.

1. Navigate to **Administrative Tools** | **Discovery**.
2. Click the **Asset Discovery** tile.
3. Click **+ Add** to create a new Asset Discovery job.
4. In the **Asset Discovery** 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 Safeguard for Privileged Passwords to add the assets it discovers. You will also specify the discovery method (**Directory** or **Network Scan**).
Information tab (asset discovery)	Where you select the directory and set the search location.
Rules tab (asset discovery)	Where you define the search constraints and conditions and choose the profile you want to govern the discovered assets.
Schedule tab (asset discovery)	Where you configure the schedule for the discovery job.
Summary tab (asset discovery)	Where you review the Asset Discovery job parameters and save it.

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 **Administrative Tools** | **Discovery** | **Asset Discovery** | (add or edit a Asset Discovery job).

On the **Asset Discovery** dialog, **General** tab, supply general information about the Asset Discovery job and identify the partition where you want Safeguard for Privileged Passwords to add the assets it discovers.

Table 70: 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. Limit: 255 characters
Partition	**Browse** to select the partition in which to manage the discovered assets.

Property	Description
	IMPORTANT: You cannot change the partition after you save this discovery job.
Method	Choose a type of discovery: • **Network Scan** • **Directory** If you select **Directory**, directory assets that are shared can be discovered into any partition. Directories include Active Directory or OpenLDAP. 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.

Information tab (asset discovery)

Navigate to **Administrative Tools** | **Discovery** | **Asset Discovery** | (add or edit a Asset Discovery job).

On the **Asset Discovery** dialog, **Information** tab, define the directory or network information for the discovery job.

Table 71: Discovery: Information properties for Directory scans

Property	Description
Directory	Select the **Directory** on which to run the Asset Discovery job.

Table 72: 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.
IPv4 Range	Enter a range of IPv4 addresses to scan: • **Starting IP Address** • **Ending IP Address** Click **+ Add** or **− Delete** to add or remove IPv4 address range sets.

Property	Description
Advanced	
Exclude IP	Safeguard for Privileged Passwords 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.

Rules tab (asset discovery)

Navigate to **Administrative Tools** | **Discovery** | **Asset Discovery** | (add or edit a Asset Discovery job)

Use the **Rules** tab on the **Asset Discovery** dialog to govern the discovered assets.

Discovery details

- Once Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 **Rules** tab, click **+ Add**.
2. In the **Asset Discovery Rule** dialog, enter a **Name** up to 50 characters.
3. You must specify at least one condition, the connection, and a profile for each rule:
   a. Under **Settings**, click Add Condition (asset discovery) to add one or more **Group**, **Constraints**, **LDAP Filter** (for LDAP or Active Directory), or **Find All**.

      Once one or more conditions have been added, you can **Edit** or **Delete** existing conditions.

   b. A **Connection Template** is required and defaults to **None** (no credentials are associated). To change this, select **Edit** to configure the authentication parameters. For more information, see Edit Connection Template (asset discovery) on page 242.

   c. For **Asset Profile**, you can **Edit** or **Delete** the profile to govern the discovered assets. The asset profile defaults to the partition default profile and is based on the partition selected on the General tab (asset discovery).

d. Select **Add Account Discovery Job** to select a schedule.

e. For **Managed Network**, you can **Edit** or **Delete** the managed network assigned for workload balancing.

4. Click **OK** 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 Safeguard for Privileged Passwords runs the discovery job, it finds all assets that meet all of the search conditions.

Navigate to **Administrative Tools** | **Discovery** | **Asset Discovery** | (add or edit a Asset Discovery job) | **Asset Discovery** dialog | **Rules** tab | **Asset Discovery Rule** dialog | **Add Condition**.

Add Find All condition

1. In the **Condition** dialog, in **Find By**, choose **Find All**.
2. 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.
3. 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.
4. Click **OK.**

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. (Optional) Select **Include objects from sub containers** to discover assets in sub-containers.
4. 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 operation:

- **Equals**
- **Not Equals**
- **Starts With**
- **Ends With**
- **Contains**

c. In the text box, type a value of up to 255 characters. The search is case-sensitive and does not allow wild cards.

5. 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.
6. 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.
7. Click **OK** to save your selections.

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.

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.

Edit Connection Template (asset discovery)

You can change how you want Safeguard for Privileged Passwords to connect to and communicate with the discovered assets. The default **Connection Template** is **None** so assets are authenticated manually.

Navigate to **Administrative Tools** | **Discovery** | **Asset Discovery** | (add or edit a Asset Discovery job) | **Asset Discovery** dialog | **Rules** tab | **Asset Discovery Rule** dialog | **Connection Template**.

Discovery details

- Once Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 **Asset Discovery Rule** dialog, click ✎ **Edit** next to **Connection Template**.
2. In the **Connection Template** dialog, **Product** defaults to **Use Discovered Platform**. You can select a different product and may need to completed additional information based on the product selected.
3. Select an **Authentication Type:**
   - **SSH Key**: To authenticate to the asset using an SSH authentication key.
     - **Browse** to select an SSH Key and provide the service **Service Account Name**.

    - You can edit or remove the **Service Account Profile**. 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.
    - Under **Service Account Name**, click **Select Account** to choose the directory account. The **Service Account Profile** for the directory account displays for reference.
    - You can edit or remove the **Service Account Profile**. 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.
    - Enter the **Service Account Name** and **Password**.
    - You can edit or remove the **Service Account Profile**. Available profiles are based on the partition selected on the General tab (asset discovery).
  - **None**: The accounts associated with the asset are not managed and no asset related credentials are stored.

4. Click **Advanced** to enter settings if you selected one of these authentication types: **SSH Key**, **Directory Account**, or **Password**. If you selected **None**, the **Advanced** settings are not needed and are ignored, if entered.
   - **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 passwords and to discover accounts.
   - **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**: The session timeout period.
   - **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 Safeguard for Privileged Passwords 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 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 Certificates store. Only clear the **Verify SSL Certificate** option if you do not want to establish trust with the asset's certificate in Safeguard for Privileged Passwords's Trusted 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**: 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.

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, Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 **Administrative Tools** | **Discovery** | **Asset Discovery** | (add or edit a Asset Discovery job) | **Asset Discovery** dialog | **Rules** tab | **Asset Discovery Rule** dialog | **Asset Profile**.

To edit the asset profile information

1. Click ✎**Edit** next to **Asset Profile**.
2. **Browse** to 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 **OK** to save your selection.

Schedule tab (asset discovery)

From the **Asset Discovery** dialog, **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.)

- 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.

  - **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 - delete 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 AM**
- **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 that 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 20:00:00 PM** and **Repeat 2**.

- **Time Zone**: Select the time zone.

Summary tab (asset discovery)

From the **Asset Discovery** dialog, **Summary** tab, review the Asset Discovery job parameters and save it.

1. Review the following settings:
   - **Method**
   - **Information**
   - **Rules**
   - **Schedule**
2. Modify the Asset Discovery job settings, if necessary.
3. Click **OK** to save the discovery job.

Editing an Asset Discovery job

You can change the settings for an Asset Discovery job.

1. Navigate to **Administrative Tools** | **Discovery**.
2. Click the **Asset Discovery** tile.
3. Select an Asset Discovery job.

4. Click **Edit** to update the selected Asset Discovery job. For more information, see Adding an Asset Discovery job on page 236.
5. Make the updates.
6. Click **OK**.

Deleting an Asset Discovery job

You can delete an Asset Discovery job.

1. Navigate to **Administrative Tools** | **Discovery**.
2. Click the **Asset Discovery** tile and 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.

1. Navigate to **Administrative Tools** | **Discovery** and click the **Asset Discovery Results** tile.
2. On the **Asset Discovery Results** grid:
   - Click **Refresh** to refresh the results.
   - 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.
3. Click **Search** and enter the character string to be used to search for a match. For more information, see Search box on page 111.
4. Click a column to sort the column information displayed for each job:
   - **User**: The user who ran the job or **Automated System**, if the job is run on an automated schedule
   - **Date**: The most recent date the Asset Discovery job successfully ran
   - **Job Name**: The name of the Asset Discovery job
   - **Type**: The type of Asset Discovery job (for example, **Network Scan** or **Directory Scan**)
   - **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 Safeguard for Privileged Passwords Appliance
- **Directory**: If applicable, the name of the directory on which the Asset Discovery job ran
- **# Assets Found**: The number of asset found during the discovery job

5. For additional detail on an Asset Discovery job result, double-click the result row to view the **Asset Discovery Results** pop-up window. On this window, click **# of Assets Found** to see a list of the assets.

Account Discovery

Account Discovery jobs include the rules Safeguard for Privileged Passwords 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 156.

To configure and schedule Account Discovery jobs, perform one of the following:

- You can create or edit an Account Discovery job from **Administrative Tools** | **Discovery** | **Account Discovery**. 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 on page 193.

Supported platforms

Safeguard for Privileged Passwords supports account discovery on the following platforms:

- AIX
- HP-UX
- Linux / Unix (based)
- MAC OS X
- Solaris
- Windows (services and tasks)

Properties and toolbar

Navigate to **Administrative Tools** | **Discovery** | **Account Discovery**.

Use these toolbar buttons to manage the Account Discovery jobs.

Table 73: Account Discovery: Toolbar

Option	Description
Add	Add an Account Discovery job. For more information, see Adding an Account Discovery job on page 251.
Delete Selected	Delete the selected Account Discovery job.
Refresh	Update the list of Account Discovery jobs.
Edit	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.
Details	View additional details about the selected Account Discovery job.
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.
Search	Enter the character string to be used to search for a match. For more information, see Search box on page 111.

Account Discovery jobs display in the grid.

Table 74: Account Discovery: Account Discovery job grid

Name	Name of the discovery job
Creator	Indicates the source of the job, for example, Automated System or a specific administrator.
Discovery Type	The type of discovery performed, 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 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.
Asset Count	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.

Double-click on an Account Discovery job to view the details.

Table 75: Account Discovery tab properties

Partition	The partition on which the Account Discovery job runs
Name	The name of the Account Discovery job
Description	The description of the Account Discovery job
Discovery Type	The type platform, for example, Windows, Unix, or Directory
Directory	If applicable, the directory on which the selected Account Discovery job runs
Schedule	The interval for the Account Discovery job to run
Rules	• **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 254. • **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 Safeguard for Privileged Passwords. • **Set default password**: A check mark displays if the rule causes default passwords to be set automatically. • **Assign to Profile**: The partition profile assigned • **Assign to Sync Group**: A check mark displays if the rule automatically associated the accounts with a password 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.

Account Discovery job workflow

Safeguard for Privileged Passwords's Account Discovery jobs discover accounts of the assets that are in the scope of a partition profile. For more information, see About partition profiles on page 293. 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.
   - To create an Account Discovery job then add assets. For more information, see Adding an Account Discovery job on page 251.
   - To create an asset and associate an Account Discovery job. For more information, see Adding an asset on page 193.
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 **Assets**, right-click the asset and choose to run the account or service discovery.
   - From **Discovery** | **Account Discovery** click **Discover Accounts** or **Discover Services**.
   - From **Assets** | **Discovered Services** click **Discover Services**. For more information, see Discovered Services tab (asset) on page 190.
3. After the Account Discovery job runs, you can mark the managed accounts from **Administrative Tools** | **Discovery** | **Discovered Accounts**.
   - Click **Disable** to prevent Safeguard for Privileged Passwords from managing the selected account.
   - Click **Enable** to manage the selected account and assign it to the scope of the default profile.

   NOTE: The discovery job finds all accounts that match the discovery rule's criteria regardless of the state and reports only the accounts discovered that do not currently exist. Account Discovery does not update existing accounts.

Search the Activity Center for information about discovery jobs that have run. Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords performs

account discovery. For more information, see Account Discovery job workflow on page 251.

To add an Account Discovery job

1. Navigate to **Administrative Tools** | **Discovery** | **Account Discovery**.
2. Click **+ Add** to open the **Account Discovery** dialog.
3. Provide the following:
   a. **Partition**: **Browse** to select a partition.
   b. **Name**: Enter a name for the account discovery job. Limit: 50 characters.
   c. **Description**: Enter descriptive text about the account discovery job. Limit: 255 characters
   d. **Discovery Type**: The platform, for example, Windows, Unix, or Directory. Make sure the Discovery Type is valid for the assets associated with the Partition selected earlier on this dialog.
   e. **Directory**: If the **Discovery Type** is **Directory**, select the directory on which the Account Discovery job runs.
   f. Click the **Schedule** button and choose an interval for to run the Account Discovery job.

      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.

        - **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 **-** delete 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 AM**
  - **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 that 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 20:00:00 PM** and **Repeat 2**.

- **Time Zone**: Select the time zone.

g. **Rules**: You can add, delete, edit or copy rules. For more information, see Adding an Account Discovery rule on page 254.

h. **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 and can be viewed in by clicking the **Discovered Services** tile. For more information, see Discovered Services on page 262.

   For more information, see Adding an Account Discovery job on page 251.

   Automatically Configure Dependent Systems: (For Windows accounts only and deselected by default.) 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. The dependencies are listed on **Administrative Tools** | **Assets** | **Account Dependencies**. If you clear the check box and run the account discovery job again, the dependencies are not removed. Dependencies can be manually removed from **Administrative Tools** | **Assets** | **Account**

Dependencies. For more information, see Account Dependencies tab (asset) on page 188.

4. Click **OK**.
5. 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 198.
   - 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 248.

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. On the **Account Discovery** dialog, click **+ Add Discovery Rule** to open the **Account Discovery Rule** dialog.
2. **Name**: Enter a unique name for the account discovery rule. Limit: 50 characters.
3. **Find By**: Select one of the types of search below.
   If the **Discovery Type** on the previous **Account Discovery** dialog is Windows or Unix, you can search by **Property Constraint** 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**.

- **Property Constraint**: Select this option to search for accounts based on an account's property. Available Unix properties are GID, UID, Name, and Group. Available Windows and Directory properties are RID, GID, UID, Name, and Group. All are limited to 255 numeric characters.

  IMPORTANT: Some **Property Constraint** selections may give slow results. Using **Group** is especially discouraged.

    - Selections:
        - **RID (ranges)**: RID property only applies to Windows and Microsoft Active Directory. Enter one or more Relative Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example,

type in **1000** and press Enter. Then type in **5000-7000** and press Enter. The selections display and can be deleted. Spaces and commas are not allowed.

- **GID (ranges)**: Enter one or more Group Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example, type in **8** and press **Enter**. Type in **10-12** and press **Enter**. The selections display and can be deleted. Spaces and commas are not allowed.
- **UID (ranges)**: Enter one or more User Identifier numbers. To enter multiple IDs or ID ranges, you must enter each element of the list separately. For example, type in **1** and press Enter. Then type in **5-7** and press Enter. The selections display and can be deleted. Spaces and commas are not allowed.
- **Name (ranges)**: Using **Name (ranges)** is discouraged as it may slow your results. It is recommended you use **Name** (described earlier) to search by account name. For an OpenLDAP 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 597.
- **Group (ranges)**: Using **Group (ranges)** is discouraged as it may slow your results. It is recommended you use **Group** (described earlier) to search by group name. For an OpenLDAP 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 597.

- 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**.

- **LDAP Filter**: Select this option to search for accounts using an LDAP query. Type an LDAP query into the field.
- **Find All**: This option is selected by default and will find all accounts based on the rules.

- 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**.

4. **Automatically Manage Found Accounts**: Select to automatically add the discovered accounts to Safeguard for Privileged Passwords. When selected, you can select **Set default password** then enter the password.
5. **Assign to Sync Group**: Click **Browse** to select a password sync group to control password validation and reset across all associated accounts. For more information, see Password sync groups on page 432.
6. **Assign to Profile**: If a profile was not automatically assigned for a sync group (previous step), click **Browse** to select a profile to identify the configuration settings for the discovered accounts. About partition profiles.
7. **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.
8. **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 he or she is an authorized user.
9. (For directory accounts only) **Available for use across all partitions**: 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.
10. Click **OK**. The **Accounts Discovery** dialog displays a list of the rules for this Account Discovery job.
11. Click **OK** to save the Account Discovery job.

Editing an Account Discovery job

Changing the assets associated with an Account Discovery job

To change the assets associated with an Account Discovery job, perform on of the following:

- From Account Discovery:
  1. Go to **Administrative Tools** | **Discovery** | **Account Discovery**.
  2. Select the Account Discovery job.
  3. Click **Occurrences**.
  4. Add the asset to the job.
- From Assets:
  1. Go to **Administrative Tools** | **Assets**.
  2. Click the the asset.
  3. On the **General** tab, go to **Account Discovery** and click **Edit**.
  4. In the **Description** drop-down, select the Account Discovery job. For more information, see Account Discovery tab (add asset) on page 198.
- From Partitions:
  1. Go to **Administrative Tools** | **Partitions**.
  2. Select the partition.
  3. Click the **Assets** tab.
  4. From the list of assets in the partition, double-click the asset.
  5. Scroll to **Account Discovery** and click **Edit**.
  6. In the **Description** drop-down, select the Account Discovery job. For more information, see Account Discovery tab (add asset) on page 198.

Changing the settings for an Account Discovery job

You can change the settings for an Account Discovery job

1. Navigate to **Administrative Tools** |**Discovery**.
2. Click the **Account Discovery** tile.
3. Select an Account Discovery job.
4. Click **Edit** to update the selected Account Discovery job. For more information, see Adding an Account Discovery job on page 251.
5. Make the updates.
6. Click **OK**.

Deleting an Account Discovery job

You can delete an Asset Discovery job.

1. Navigate to **Administrative Tools** |**Discovery**.
2. Click the **Asset Discovery** tile.
3. Click **Delete** to delete the selected Asset Discovery job.
4. Click **OK**.

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

1. Navigate to **Administrative Tools** | **Discovery** and click the **Account Discovery Results** tile.
2. On the **Account Discovery Results** grid:
   - Click **Refresh** to refresh the results.
   - 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.
3. Click **Search** and enter the character string to be used to search for a match. For more information, see Search box on page 111.
4. View the following information displays for each job:
   - **User**: The user who ran the job or **Automated System**, if the job is run on an automated schedule.
   - **Date**: The most recent date the Account Discovery job successfully ran.
   - **Asset**: The asset which is associated with the Account Discovery job.
   - **Event**: The outcome of running the Account Discovery job event, which may be **Account Discovery Succeeded**, **Account Discovery Failed**, or **Account Discovery Started**.
   - **Partition**: The partition in which the discovered accounts will be managed.
   - **Profile**: The partition profile which will govern the discovered accounts.
   - **Account Discovery Job**: Name of the discovery schedule.
   - **Appliance**: The name of the Safeguard for Privileged Passwords Appliance.
   - **# Accounts Found**: The number of accounts found during the discovery job.

5. For additional detail on an Account Discovery job result, double-click the result row to view the **Account Discovery Results** pop-up window. On this window, click **# of Accounts Found** to see a list of the accounts.

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 Management tab (add asset) on page 195.

Navigate to **Administrative Tools** | **Discovery** | **Discovered Accounts** tile.

Use these toolbar buttons to manage the discovered accounts.

Table 76: Discovery: Discovered Accounts toolbar

Option	Description
Partition	Select the partition associated with the discovered accounts you want to view.
Manage	Select **Manage** to have Safeguard for Privileged Passwords manage an account with no (blank) status or accounts with a status of **Disabled**. The **Disabled** status is displayed when a discovered account was set to **Managed** then **Ignored**.
Ignore	Select **Ignore** to set the **Status** to **Ignore** to prevent Safeguard for Privileged Passwords from managing the selected account. An ignored account is not unconfigured as a dependent account. If you choose to **Manage** the asset later, Safeguard for Privileged Passwords reenables recognition of all the associated accounts.
Show Ignored	Display the accounts with a **Status** of **Ignored** (disabled).
Hide Ignored	Hide the accounts with a **Status** of **Ignored** (disabled).
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 111.

The following information displays.

Table 77: Discovery: Discovered Accounts properties grid

Property	Description
Status	The discovered account may be: • **Managed**: A discovered account that is managed • Blank (no value): 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
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
Domain Name	The domain name of the account if the account is an Active Directory account.
Account Name	The account to which the account is associated.
Account Discovery Job	Name of the discovery schedule.
Asset Discovery Rule	The name of the Asset Discovery rule applied to discover 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 **Discovery 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 on page 251.

Viewing Service Discovery Results

Service Discovery is configured on an Account Discovery job but runs separately. You can view the results of service discovery by time frame.

1. Navigate to **Administrative Tools** | **Discovery** and click the **Service Discovery Results** tile.

2. On the **Service Discovery Results** grid:
   - Click **Refresh** to refresh the results.
   - 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.
3. Click **Search** and enter the character string to be used to search for a match. For more information, see Search box on page 111.
4. View the following information displays for each job:
   - **User**: The user who ran the job or **Automated System**, if the job is run on an automated schedule.
   - **Date**: The most recent date the Account Discovery job successfully ran.
   - **Asset**: The asset that is associated with the discovery job.
   - **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.
   - **Partition**: The partition in which the discovered service accounts will be managed.
   - **Profile**: The partition profile that will govern the discovered service accounts.
   - **Account Discovery Job**: Name of the discovery schedule.
   - **Appliance**: The name of the Safeguard for Privileged Passwords Appliance.
   - **# Accounts Found**: The number of service accounts found during the discovery job.
5. For additional detail on a Service Account Discovery job result, double-click the result row to view the **Service Account Discovery Results** pop-up window. On this window, click **# of Accounts Found** to see a list of the accounts.

Discovered Services

The **Discovery** | **Discovered Services** tile displays information for the selected partition on which the services were discovered. If desired, dependencies must be manually removed.

The Asset Administrator or delegated administrator can configure service discovery jobs to scan Windows assets and discover Windows services and tasks that may require authorization credentials. 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.

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 or task was discovered. For more information, see Adding an Account Discovery job on page 251.
- You can manually run a Service Discovery job from **Administrative Tools** | **Assets** | **Discovered Services**. For more information, see Discovered Services tab (asset) on page 190.

Discovered services and tasks association to known Safeguard accounts

Service discovery jobs associate Windows services and tasks with accounts that are already managed by Safeguard for Privileged Passwords. The accounts put under management display with an **Account Status** of **Managed**. When the account's password is changed by Safeguard, Safeguard updates the password corresponding to the services or tasks on the asset according to the asset's profile change settings.

Service Discovery with Active Directory

A discovered service or task configured to use Active Directory authentication 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 254.

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

Navigate to **Administrative Tools** | **Discovery** | **Discovered Services** tile.

Use these toolbar buttons to manage the discovered services.

Table 78: Discovery: Discovered Services toolbar

Option	Description
Partition	Select the partition for the discovered services.
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 260.

Option	Description
Show Ignored	Display the accounts with a **Status** of **Ignored**.
Hide Ignored	Hide the accounts with a **Status** of **Ignored**.
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 111.

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** or **Task**).

Table 79: Discovery: Discovered Services properties

Property	Description
Asset Name	The name of the asset where the service or task 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.
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 260. The discovered account may be: • **Managed**: A discovered account that is managed • Blank (no value): 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
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 partition profile that is associated to the asset.

Property	Description
	For more information, see Adding an Account Discovery job on page 251.
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 on the target machine. If there is no check mark, the service or task is disabled on the target machine.
Service Ignored	Ignored means the service or task will not show up in the grid. In other words, the service or task 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 or task was discovered.

18

Entitlements

A Safeguard for Privileged Passwords 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 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.

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 add users or user groups.

Go to **Administrative Tools** and click **Entitlements**. The **Entitlements** view displays.

If there are one or more invalid or expired policies, a **Warning** and message like `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 on page 269.

The following information displays about the selected entitlement:

- General tab: Displays the general and time restriction settings information for the selected entitlement.
- Users tab: 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 join and was assigned and used by a Sessions Appliance. The certificate users created during the join can be added to the **Users** tab but are not there by default.
- Access Request Policies tab: Displays the access request policies that govern the accounts or assets in the selected entitlement, including session access policies.
- History tab: Displays the details of each operation that has affected the selected entitlement.

Use these toolbar buttons to manage entitlements.

- **Add Entitlement**: add entitlements to Safeguard for Privileged Passwords. For more information, see Adding an entitlement on page 273.

- **Delete Selected**: Remove the selected entitlement. For more information, see Deleting an entitlement on page 290.
- **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 111.

Related Topics

Adding an entitlement

Modifying an entitlement

Creating an access request policy

Modifying an access request policy

Deleting an access request policy

General tab

The **Administrative Tools** | **Entitlements** | **General** tab lists information about the selected entitlement.

Large tiles at the top of the tab display the number of **Users**, **Accounts**, and **Assets** associated with the selected entitlement. Clicking a tile heading opens the corresponding tab.

Table 80: Entitlements General tab: General properties

Property	Description
Name	The entitlement name.
Priority	A unique number that determines the processing order of the entitlement in relation to other entitlements. For more information, see About priority precedence on page 274.

Table 81: Entitlements General tab: Time restrictions properties

Property	Description
Time Restrictions	The days and times this entitlement is in effect. For more information, see About time restrictions on page 276.
Expires	The day and time this entitlement expires.

Description: Information about the selected entitlement.

Related Topics

Modifying an entitlement

Users tab

The **Administrative Tools** | **Entitlements** | **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 join and was assigned and used by a Sessions Appliance. The certificate users created during the join can be added to the **Users** tab but are not there by default.

Click **+ Add User or User Group** from the details toolbar to add one or more requester users or user groups to the selected entitlement.

Table 82: Entitlements: User tab properties

Property	Description
Type	Type of member: • Group • User
Name	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.
Domain Name	If applicable, the name of the domain of the user group or user

Use these buttons on the details toolbar to manage the requester users associated with the selected entitlement.

Table 83: Entitlements: Users tab toolbar

Option	Description
+ Add User or User Group	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 287.

Option	Description
Remove Selected	Remove the selected user or user group from the entitlement.
Refresh	Update the list of requester users or user groups.
Details	View additional details about the selected user or user group.
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 111.

Related Topics

Adding users or user groups to an entitlement

Access Request Policies tab

The **Administrative Tools** | **Entitlements** | **Access Request Policies** tab displays the password release policies that govern the accounts in the selected entitlement.

IMPORTANT: The selection made on the **Entitlement** | **Access Request Policy** tab takes precedence over the selections on **Settings** | **Cluster** | **Managed Networks** page. If a **Managed Networks** rule includes nodes from different SPS clusters, SPP will only select the nodes from the same cluster that was assigned on the **Session Settings** page of the **Access Request Policy** tab.

Click **+Create Access Policy** from the details toolbar to add a policy to the selected entitlement.

Table 84: Entitlements: Access Request Policies tab properties

Property	Description
Priority	A unique number that determines the processing order of the policy. For more information, see About priority precedence on page 274.
Name	The name of the access request policy.
Access Type	Indicates the type of access requested: • Password Release • RDP • SSH • Telnet

Property	Description
Scope	The number of unique account groups, accounts (including the number of accounts in the specified account groups), asset groups, and assets (including the number of assets in the specified asset groups) governed by the selected policy.
Description	Information about the selected policy.
Approvals	A ✔ displays if there are approver settings for the access request policy. For more information, see Approver tab on page 280.
Reviews	A ✔ displays if there are reviewer settings for the access request policy. For more information, see Reviewer tab on page 282.
Emergency	A ✔ displays if a user can request emergency access to the accounts and assets governed by the policy. **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.For more information, see Emergency tab on page 286.
Time Restrictions	A ✔ displays if time restrictions are specified for access requests for accounts and assets governed by the policy. For more information, see Time Restrictions tab on page 286.
Expired	A ⚠**Warning** displays for the entitlement when it contains at least one expired policy. You can configure Safeguard for Privileged Passwords to notify you of an impending entitlement or policy expiration by sending an event notification to a syslog server, in an email message, or a SNMP trap. For more information, see External Integration settings on page 381.
Invalid	A ⚠**Warning** displays for the entitlement when it contains at least one invalid policy. Check the following if there is an invalid policy. • Validate that the SPS cluster is still joined to SPP. • Validate the SPS cluster is available. • Validate there are no network issues that prevent SPP from communicating with SPS. • Validate SPP can communicate with the SPS cluster. • Validate that the assigned session connection policy is on the SPS cluster master.

Property	Description
	• Validate the session connection policy is still compatible with SPP given what the administrator changed. For more information, see Managed networks on page 369.

Use these buttons on the details toolbar to manage your access request policies.

Table 85: Entitlements: Access Request Policies tab toolbar

Option	Description
Create Access Policy	Add an access request policy to the selected entitlement. For more information, see Creating an access request policy on page 276.
Delete Selected	Remove the selected policy from the selected entitlement. For more information, see Deleting an access request policy on page 288.
Refresh	Update the list of access request policies.
Edit Access Policy	Modify the selected policy. For more information, see Modifying an access request policy on page 289.
Copy Access Policy	Make a copy of the selected policy. For more information, see Copying an access request policy on page 289.
Details	View additional details about the selected policy. For more information, see Viewing and editing policy details on page 289.
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 111.

History tab

The **Administrative Tools** | **Entitlements** | **History** tab allows you to view or export the details of each operation that has affected the selected entitlement.

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.
- **Search**: For more information, see Search box on page 111.

- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Table 86: 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

Select an event to display this additional information for some types of events (for example, create and update events).

Table 87: Additional History tab properties

Property	Description
Property	The property that was updated
Old Value	The value of the property before it was updated
New Value	The new value of the property

Managing entitlements

Use the controls and tabbed pages on the **Entitlements** page to perform the following tasks to manage Safeguard for Privileged Passwords entitlements:

- Adding an entitlement
- Adding users or user groups to an entitlement
- Creating an access request policy
- Deleting an access request policy
- Modifying an access request policy
- Copying an access request policy
- Viewing and editing policy details
- Modifying an entitlement
- Deleting an entitlement

Adding an entitlement

It is the responsibility of the Security Policy Administrator to add entitlements to Safeguard for Privileged Passwords.

To add an entitlement

1. Navigate to **Administrative Tools** | **Entitlements**.
2. Click **+ Add Entitlement** from the toolbar.
3. In the **Entitlement** dialog, provide information in each of the tabs:

General tab	Where you add general information about the entitlement
Time Restrictions tab	Where you indicate entitlement time restrictions

Related Topics

Adding users or user groups to an entitlement

General tab

Navigate to **Administrative Tools** | **Entitlements**| (add or edit entitlement).

On the General tab, specify the following information about the entitlement.

Table 88: Entitlement: General tab properties

Property	Description
Name	Enter a unique name for the entitlement. Limit: 50 characters
Description	Enter descriptive text about the entitlement. Limit: 255 characters
Priority	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 About priority precedence on page 274.

About priority precedence

An entitlement defines which users are authorized to check out passwords for accounts in the scope of its 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. Safeguard for Privileged Passwords uses both entitlement and policy priorities to determine which policy to use for a password release. Safeguard for Privileged Passwords first considers the entitlement priority, then the priorities of access request policies within that entitlement.

Example scenario:

- Entitlement A (priority 1)
  - Policy: Week Day Policy.
    - Policy time restrictions: Monday through Friday 8:00 a.m. to 5:00 p.m.
    - Scope: AccountX
- Entitlement B (priority 2)
  - Policy 1: Sunday AM (priority 1)
    - Policy time restrictions: Sunday 8:00 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 4 p.m., Safeguard for Privileged Passwords 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.

Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords grants the request.

To change an entitlement's priority

1. Select the priority number in the entitlement list.
2. Enter another number.

To modify a policy's priority

1. In **Entitlements**, select an entitlement and switch to the **Access Request Policies** tab.
2. Double-click a policy, or select a policy and click **Edit Access Policy**.
3. Enter or select a new priority number.
4. Click the **Refresh** button.

Time Restrictions tab

Time restrictions control when the entitlement is in effect relative to the user's time zone. For more information, see About time restrictions on page 276.

On the Time Restrictions tab, specify the time restriction properties for the entitlement.

Navigate to **Administrative Tools** | **Entitlements**| (add or edit entitlement).

Table 89: Entitlement: Time Restrictions tab properties

Property	Description
Use Time Restrictions	Select this option to enforce time restrictions.
Daily calendar	Select and drag the hours you want to allow.
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.

About time restrictions

An entitlement's time restrictions enforce when Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords enforces the policy in the user's time zone set in his account profile.

Creating an access request policy

It is the responsibility of the Security Policy Administrator to define access request policies in Safeguard for Privileged Passwords.

A policy defines:

- The scope, which may be assets, asset groups, accounts, or account groups.
- The access type, which may be password, SSH, RDP (remote desktop), or 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. You cannot copy an access request policy and add it to another entitlement; access request policies are entitlement-specific.

To add an access request policy to an entitlement

1. Navigate to **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement from the object list and open the **Access Request Policies** tab.
3. Click **+ Create Access Policy** from the details toolbar.
4. In the **Access Request Policy** dialog, provide information in each of the tabs:

General tab	Where you add general information about the access request policy as well as specify the type of access being requested

Scope tab	Where you assign assets, asset groups, accounts, or account groups to an access request policy
Requester tab	Where you configure the access request policy requester settings
Approver tab	Where you configure the access request policy approver settings
Reviewer tab	Where you configure the access request policy reviewer settings
Access Config tab	Where you define the access settings for the selected type of request including allowing users to request passwords from their respective linked accounts
Session Settings tab	Where you configure the recording settings for session access requests
Time Restrictions tab	Where you indicate policy time restrictions
Emergency tab	Where you enable emergency access for the accounts governed by the access request policy

Related Topics

Deleting an access request policy

Modifying an access request policy

Copying an access request policy

Viewing and editing policy details

Reasons

General tab

On the General tab, enter the following information for the access request policy.

Navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy).

Table 90: 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.

Property	Description
	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 About priority precedence on page 274.
Access Type	Specify the type of access being requested: • Password • RDP • SSH • Telnet NOTE: You can configure an access request policy for a password release, however, if the Privileged Passwords module license is not installed, you will not be able to submit a password release request. Similarly, you can configure an access request policy for a session request.
Have the Policy Expire on Date and Time	If applicable, select this check box to enforce an expiration date for the policy. Enter the expiration date and time.

Scope tab

Use the Scope tab to assign accounts, account groups, assets, and asset groups to an access request policy.

Navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy).

1. On the **Scope** tab:
    1. Click **+ Add** from the details toolbar and select one of the following options:
        - **Add Account Group**
        - **Add Account**
        - **Add Asset Group**: Only available for a session access request (that is, when access type **RDP**, **SSH**, or **Telnet** is selected on the General tab.
        - **Add Asset**: Only available for a session access request (that is, when access type **RDP**, **SSH**, or Telnet is selected on the General tab.

2. In the selection dialog, make a selection then click **OK**.

   If you do not see the selection you are looking for, depending on your Administrator permissions, you can create it in the selection 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.)

2. 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**.

Requester tab

Use the **Requester** tab to configure the requester settings for an access request policy.

Navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy).

Table 91: Access Request Policy: Requester tab properties

Property	Description
Reasons	Click **+Select Reason** to add one or more reasons to the selected access request policy. Then, when requesting access to a password 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 Safeguard for Privileged Passwords to use this option. For more information, see Reasons on page 312. If you do not see the reason you are looking for, you can create a reason from the **Reasons** selection dialog by clicking the **+Create New** toolbar button.
Require Reason	Select this check box 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.
Require Comment	Select this check box to require that a requester provide a **Comment** when making an access request.
Require Ticket Number	Select this check box to require that a requester provide a ticket number when making an access request. The ticket number can be defined and not validated against an external ticketing system but, optionally, may be validated against

Property	Description
	the regular expression of a generic ticketing system. The ticket number is used to approve a password or session request and is tracked through the Activity Center. You can validate the ticket against your company's external ticket system, such as ServiceNow, or Remedy, or another ticketing system. To do this, you must have the ticketing system configured in Safeguard for Privileged Passwords to use this option. For more information, see Ticketing systems on page 417.
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 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.

Approver tab

Use the **Approver** tab to specify the approver settings for an access request policy.

Navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy).

Table 92: 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 Safeguard for Privileged

Property	Description
	Passwords users, you can use the ⊗ **Clear** icon to remove an individual address from this list or right-click and select **Remove All** to clear all addresses from the list. NOTE: To send event notifications to a user, you must configure Safeguard for Privileged Passwords to send alerts. For more information, see Configuring alerts on page 118.
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 assets governed by this policy. Use the ⊗**Clear** icon to remove an individual approver user or user group from this list or right-click and select **Remove All** to clear all users from the list. Click **+ Add** 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords user. You can enter email addresses for non-Safeguard for Privileged Passwords users.

Property	Description
	If you used the **To** button to add Safeguard for Privileged Passwords users, you can use the ⊗ **Clear** icon to remove an individual address from this list or right-click and select **Remove All** to clear all addresses from the list. IMPORTANT: Safeguard for Privileged Passwords does not dynamically maintain the email addresses for an escalation notification contact list. If you change a Safeguard for Privileged Passwords user's email address or delete a Safeguard for Privileged Passwords 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 559. NOTE: To send event notifications to a user, you must configure Safeguard for Privileged Passwords to send alerts. For more information, see Configuring alerts on page 118.
Approval Anywhere has been enabled. View enabled users.	Indicates that the Approval Anywhere feature has been configured. 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 Approval Anywhere approvers by clicking the **+Add** toolbar button in the **Approval Anywhere Users** dialog.

Reviewer tab

Use the **Reviewer** tab to define the reviewer settings for an access request policy.

Navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy).

Table 93: 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. • **Reviewers**: **Browse** to select one or more users or groups of users who can review access requests for accounts and assets governed by this policy.

Property	Description
	Use the ⊗**Clear** icon to remove an individual reviewer user or user group from this list or right-click and select **Remove All** to clear all users from the list. NOTE: A reviewer can only review an access request once it is completed. 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. NOTE: The users you authorize as reviewers receive alerts when an access request requires their review if they have Safeguard for Privileged Passwords configured to send alerts.
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 Safeguard for Privileged Passwords user. If you used the **To** button to add Safeguard for Privileged Passwords users, you can use the ⊗ **Clear** icon to remove an individual address from this list or right-click and select **Remove All** to clear all addresses from the list. NOTE: You can enter email addresses for non-Safeguard for Privileged Passwords users. IMPORTANT:Safeguard for Privileged Passwords does not dynamically maintain the email addresses for an escalation notification contact list. If you change a Safeguard for Privileged Passwords user's email address or delete a Safeguard for Privileged Passwords 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 559. NOTE: To send event notifications to a user, you must configure Safeguard for Privileged Passwords to send alerts. For more information, see Configuring alerts on page 118.

Access Config tab

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 **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy).

Table 94: Access Request Policy: Access Config tab properties

Property	Description
Access Type	This is a read-only field displaying the type of access selected on the General tab: • Password • SSH • RDP • Telnet
Include password release with sessions requests	If **Access Type** is SSH, RDP, or Telnet, select this check box to include a password release with session access requests.
Terminate expired sessions	If **Access Type** is SSH, RDP, or Telnet, select this check box to terminate 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. For password release requests, this option is selected by default.
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 SSH, RDP, or Telnet, select one of the following options to define the type of account credentials to be used to access the asset or account when a session is requested: • None (default): The credentials are retrieved from the vault when the session is requested. • User Supplied: The requester user must provide the credentials when the session is requested.

Property	Description
	• Linked Account: The requester user's account is linked to an asset account that will be used when the session is requested. • 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. For more information, see Linked Accounts tab (user) on page 448.

Session Settings tab

You select the one cluster or appliance to which the policy applies.

1. Navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy), then the **Session Settings** tab.
2. If you see a message like ⚠ `No SPS connection policies found.`, you may have selected a policy with an invalid connection policy. For more information, see Access Request Policies tab on page 269.
3. In **SPS Connection Policy**, select the cluster or appliance to which the policy applies.
   - The default is `safeguard_default`.
   - If you are using telnet with SPS, the telnet **Connection Policy** created in SPS is available.
   - Select `Sps Initiate` if the access policy is for use by Safeguard for Privileged Sessions (SPS) to create an SPS initiated Access Request.
     - 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.
     - For information on the SPS feature availability and use, see the *One Identity Safeguard for Privileged Sessions Administration Guide*: One Identity Safeguard for Privileged Sessions - Technical Documentation.
     - For information on the toggle to set the **Session Module Password Access Enabled**, see Session Appliances with SPS join. You will see the

following message if SPP has not been joined or the join has been deleted: `No SPS connection policies found`.

- For other policies, the host name and IP address of the cluster master is displayed first followed by the SPS cluster description.

If a policy is not functional, you will see the ⚠**Warning** icon next to a selection.

You can view the network segments that can be serviced by specific Safeguard for Privileged Passwords (SPP) or Safeguard for Privileged Sessions (SPS) Appliances within a clustered environment. For more information, see Managed networks on page 369.

Time Restrictions tab

Use the **Time Restrictions** tab to specify time restrictions for the access request policy.

Navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** | (create or edit a policy).

Table 95: Access Request Policy: Time Restriction tab properties

Property	Description
Use Time Restrictions	Select this option to specify time restrictions for access requests for accounts and assets governed by this policy. Time restrictions control when the access request policy is effective relative to the user's time zone. For more information, see About time restrictions on page 276.
Daily calendar	Select and drag the days and hours you want to allow the policy to be effective.
Reset	Click **Reset** to remove any time restrictions set in the daily calendar.

Emergency tab

Use the **Emergency** tab to enable emergency access for the accounts and assets governed by the access request policy.

Table 96: Access Request Policy: Emergency tab properties

Property	Description
Enable Emergency Access	Select this check box to allow users to request emergency access to accounts and assets governed by this policy. Clear this option to disallow emergency access.

Property	Description
	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.
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 Safeguard for Privileged Passwords user. If you used the **To** button to add Safeguard for Privileged Passwords users, you can use the ⊗ **Clear** icon to remove an individual address from this list or right-click and select **Remove All** to clear all addresses from the list. You can enter email addresses for non-Safeguard for Privileged Passwords users. To send event notifications to a user, you must configure Safeguard for Privileged Passwords to send alerts. For more information, see Configuring alerts on page 118. IMPORTANT: Safeguard for Privileged Passwords does not dynamically maintain the email addresses for an escalation notification contact list. If you change a Safeguard for Privileged Passwords user's email address or delete a Safeguard for Privileged Passwords 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 559.
Ignore Time Restrictions	This check box is selected by default, indicating that Safeguard for Privileged Passwords is to ignore time restrictions when a user requests emergency access. Clear this check box if you want to enforce the time restrictions set for this policy and only allow emergency access during the specified time period.

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 SPS join on page 377.

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 507.

To add requester users to an entitlement

1. Navigate to **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement from the object list and click the **Users** tab.
3. Click **+ Add User or User Group** from the details toolbar.
4. Select one or more users or user groups from the list in the **Users/User Groups** selection dialog, and click **OK**.

If you do not see the user or user group you are looking for, depending on your Administrator permissions, you can create them in the Users/User Groups selection dialog. (You must have Authorizer Administrator or User Administrator permissions to create users or Security Policy Administrator permissions to create user groups.)

To create new users or user groups in the Users/User Groups selection dialog

1. Click **+ Create New**, then select **Create a New User** or **Create a New User Group**.

   For more information about creating users or user groups, see Adding a user or Adding a user group.
2. Create additional users or user groups as required.
3. Click **OK** to add the new users and user groups to the selected entitlement's membership.

Deleting an access request policy

IMPORTANT: When you delete a policy, Safeguard for Privileged Passwords 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 **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement from the object list and open the **Access Request Policies** tab.
3. Select a policy.
4. Click **Delete Selected**.
5. Confirm your request.

Modifying an access request policy

Access request polices can be migrated. For more information, see Creating an access request policy on page 276.

To modify an access request policy

1. Navigate to **Administrative Tools** | **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 Access Policy**.
4. Select the view of the policy's information you want to modify (**General**, **Time Restrictions**, **Scope**, and so on).

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 **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement from the object list and open the **Access Request Policies** tab.
3. Choose a policy and click **Copy Access Policy**.
4. You must type in a unique policy name.
5. Edit the new policy's settings as desired.

Viewing and editing policy details

You must have Security Policy Administrator permissions to modify policy settings.

To view and editing the details of an entitlement's policy

1. Navigate to **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement from the object list and open the **Access Request Policies** tab.
3. Select a policy and click **Details**.

   The policy's properties dialog displays.
4. To edit the properties, double-click a property name or click the **Edit** icon to the

right of a property name (such as **General**).

The **Access Request Policies** dialog displays allowing you to make the necessary changes.

For more information, see Creating an access request policy on page 276.

Modifying an entitlement

To modify an entitlement

1. Navigate to **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement.
3. Select the view of the entitlement's information you want to modify (**General**, **Users**, or **Access Request Policies**).

   For example:

   - To change the selected entitlement's name, description, or time restrictions, double-click the **General** information on the **General** tab or click the ✎ **Edit** icon.

     NOTE: You can also double-click an entitlement name to open the **General** settings edit window.

   - To add authorized requesters to the selected entitlement, switch to the **Users** tab.

     For more information, see Adding users or user groups to an entitlement on page 287.

   - To modify an access request policy, switch to the **Access Request Policies** tab.

     For more information about access request policy details, see Creating an access request policy.

4. To view or export the details of each operation that has affected the selected entitlement, switch to the **History** tab. For more information, see History tab on page 271.

Deleting an entitlement

IMPORTANT: When you delete an entitlement, Safeguard for Privileged Passwords deletes all access request policies associated with that entitlement.

To delete an entitlement

1. Navigate to **Administrative Tools** | **Entitlements**.
2. In **Entitlements**, select an entitlement from the object list.

3. Click **Delete Selected**.
4. Enter the name of the entitlement to confirm you want to delete the entitlement.

19

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 Safeguard for Privileged Passwords. 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, Safeguard for Privileged Passwords 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 300.

You must assign all assets, and the accounts associated with them, to a partition. By default, Safeguard for Privileged Passwords assigns all assets and their associated accounts to the default partition, but you can set a different partition as the default.

Navigate to **Administrative Tools** | **Partitions** to display the following information about the selected partition.

- General 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.
- 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.
- History tab (partitions): Displays the details of each operation that has affected the selected partition.

Use these toolbar buttons to manage partitions.

- **Add Partition**: Add a partition to Safeguard for Privileged Passwords. For more information, see Adding a partition on page 300.
- **Delete Selected**: Remove the selected partition. For more information, see Deleting a partition on page 307.
- **Refresh**: Update the list of partitions.

- **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 304.
- **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 111.

About partition profiles

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

A partition can have multiple partition 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. For more information, see Adding change password settings.

When you create a new partition, Safeguard for Privileged Passwords 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 partition 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, Safeguard for Privileged Passwords 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

Safeguard for Privileged Passwords makes implicit assignments. For example, when you add an asset to Safeguard for Privileged Passwords, 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, Safeguard for Privileged Passwords implicitly adds that account to its asset's profile.

Later, if you reassign the asset to another profile, Safeguard for Privileged Passwords automatically reassigns all of the asset's associated accounts to the new profile.

Explicit associations

Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords 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 partition profile.

Related Topics

Assigning assets or accounts to a profile

Assigning a profile to an asset

Account Password Rules

How do I manage accounts on unsupported platforms

General tab (partitions)

The **General** tab lists information about the selected partition. Navigate to: **Administrative Tools** | **Partitions** | **General** tab.

Tiles above the tab display the number of **Assets**, **Accounts**, **Profiles** associated with the selected partition. Clicking a tile heading opens the corresponding tab.

Table 97: Partitions General tab: General properties

Property	Description
Name	The partition name
Delegated Owner	The users who are responsible for managing the assets and accounts in the selected partition
Description	Information about the selected partition

Related Topics

Adding a partition

Modifying a 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.

Navigate to **Administrative Tools** | **Partitions** | **Assets** tab.

Table 98: Partitions: Assets tab properties

Property	Description
Name	The asset name.
Profile	The name of the profile that manages the asset.
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 Available for discovery across all partitions on page 196.
Platform	The platform of the selected asset.
Session Request	A check in this column indicates that session access requests are enabled for the 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.
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 Connection tab (add asset) on page 200.
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 99: Partitions: Assets tab toolbar

Option	Description
Add Asset	Add one or more assets to the selected partition.
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 111.

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 partition profile, but you can reassign them. For more information, see Creating a profile on page 302.

Navigate to **Administrative Tools** | **Partitions** | **Accounts** tab.

Table 100: 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.
Profile	The name of the profile that manages the account.
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.

Property	Description
Disabled	A check in this column indicates the account is disabled.
Password	Displays ⚠ if a password is not set for the account. For more information, see Checking, changing, or setting an account password on page 165.
Description	Descriptive information entered when the account was added.

Use these buttons on the details toolbar to manage the accounts assigned to the selected partition.

Table 101: Partitions: Accounts tab toolbar

Option	Description
Refresh	Retrieve and display an updated list of assets and accounts associated with the selected partition.
Search	To locate a specific asset or account in this list, enter the character string to be used to search for a match. For more information, see Search box on page 111.

Related Topics

Adding assets to a partition

Removing assets from a partition

Profiles tab (partitions)

The **Profiles** tab lists the profiles associated with this partition. For more information, see About partition profiles on page 293.For more information, see About partition profiles on page 293.

Click **+ Create Profile** from the details toolbar to add a profile to the selected partition.

Navigate to **Administrative Tools** | **Partitions** | **Profiles** tab.

Table 102: Partitions: Profiles tab properties

Property	Description
Name	Password management profile name.
Default	"Default" displays in this column for the default profile. For more information, see Setting a default partition profile on page 305.
Check Password	The check password setting used to verify account passwords. For

Property	Description
	more information, see Check Password on page 429.
Change Password	The change password setting used to to verify account passwords. For more information, see Change Password on page 425.
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 421.
Description	Information about the selected profile.

Use these buttons on the details toolbar to manage your partitions profiles.

Table 103: Partitions: Profiles tab toolbar

Option	Description
Create Profile	Add a profile to the selected partition. For more information, see Creating a profile on page 302.
Deleted Selected	Remove the selected partition profile. If you delete a profile, Safeguard for Privileged Passwords reassigns all assets and accounts to the default profile.
Refresh	Update the list of partition profiles.
Edit Profile	Modify the selected partition profile. For more information, see Modifying a profile on page 303.
Set as Default	Set the selected profile as the default partition profile. For more information, see Setting a default partition profile on page 305.
Details	View additional details about the selected partition profile.
Search	To locate a specific partition profile or set of profiles in this list, enter the character string to be used to search for a match. For more information, see Search box on page 111.

History tab (partitions)

The **History** tab allows you to view or export the details of each operation that has affected the selected partition.

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.
- **Search**: For more information, see Search box on page 111.
- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Table 104: 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.

Select an event to display this additional information for some types of events (for example, create and update events).

Table 105: Additional History tab properties

Property	Description
Property	The property that was updated
Old Value	The value of the property before it was updated
New Value	The new value of the property

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
- Creating a profile
- Modifying a profile
- Setting a default partition profile
- Assigning assets or accounts to a profile
- Modifying a partition
- Deleting a partition
- Setting a default partition

Adding a partition

It is the responsibility of the Asset Administrator to add partitions to Safeguard for Privileged Passwords. When you create a new partition, Safeguard for Privileged Passwords creates a corresponding default profile with default schedules and rules. For more information, see Setting a default partition profile on page 305.

To add a partition

1. Navigate to **Administrative Tools** | **Partitions**.
2. Click **+ Add 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

c. **Delegated Owner**: (Optional) **Browse** to select one or more users to manage the assets and accounts in this partition.

   You can use the ⊗ **Clear** icon to remove an individual delegated owner from this list or right-click and select **Remove All** to clear all of the delegated owners from the list.

   By default, an Asset Administrator can manage all partitions; however, you can delegate partition management to a user with no administrator permissions.

When you create a new partition, Safeguard for Privileged Passwords creates a corresponding default partition profile with default schedules and rules. You can:

- Modify the profile for the partition you created. For more information, see Modifying a profile on page 303.
- Change the default partition profile. For more information, see Setting a default partition profile on page 305.

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 213.

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 partition profiles on page 293.

To add assets to a partition

1. Navigate to **Administrative Tools** | **Partitions**.
2. In **Partitions**, select a partition from the object list and open the **Assets** tab.
3. Click **+ Add Asset** from the details toolbar.
4. On the **Asset** dialog, select one or more assets.
5. Click **OK**.

If you do not see the asset you are looking for and are an Asset Administrator, you can create it in the selection dialog by clicking **+ Create New**. For more information, see Adding an asset.

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 213.

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 partition profiles on page 293.

Creating a profile

It is the responsibility of the Asset Administrator or the partition's delegated administrator to add profiles to partitions.

To add a profile to a partition

1. Navigate to **Administrative Tools** | **Partitions**.
2. In **Partitions**, select a partition from the object list and open the **Profiles** tab.
3. Click + **Create Profile** from the details toolbar.
4. 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
5. On the **Check Password** tab, select a previously defined check password setting from the drop-down menu. Check password settings are the rules Safeguard for Privileged Passwords uses to verify account passwords. Expand the **Description** to see information, if available, about the selected check password setting.
   - Click **Edit** to modify the selected check password setting.
   - Click + **Add** to create a new check password setting.

   Selecting either of these icons displays the **Check Password Settings** dialog, allowing you to specify the appropriate check password settings. For more information, see Adding check password settings on page 430.
6. On the **Change Password** tab, select a previously defined change password setting from the drop-down menu. Change password settings are the rules Safeguard for Privileged Passwords uses to reset account passwords. Expand the **Description** to see information, if available, about the selected change password setting.
   - Click **Edit** to modify the selected change password setting.
   - Click

+ **Add** to create a new change password setting.

Selecting either of these icons displays the **Change Password Settings** dialog, allowing you to specify the appropriate change password settings. For more information, see Adding change password settings on page 426.

7. On the **Account Password Rules** tab, select a previously defined account password rule. An account password rule is a complexity rule that governs the construction of the new password created by Safeguard for Privileged Passwords during an automatic password change. Expand the **Description** to see information, if available, about the selected account password rule.

   - Click **Edit** to modify the selected account password rule.
   - Click + **Add** to create a new account password rule.

   For more information, see Adding an account password rule on page 422.

8. Click to save your selections and create the partition profile.

When creating a new partition profile, the **Password Sync Groups** tab is not displayed. This tab is displayed while editing a partition profile. For more information, see Modifying a profile on page 303. You can use the **Password Sync Groups** tab to add or update a password sync group governed by the partition profile change schedule. For more information, see Password sync groups on page 432.

Related Topics

Assigning assets or accounts to a profile

Setting a default partition profile

Assigning a profile to an asset

Account Password Rules

Modifying a profile

Any modifications that you make to a profile affects all the assets and accounts governed by that profile.

To modify a profile

1. Navigate to **Administrative Tools** | **Partitions**.
2. Select a partition from the object list and open the **Profiles** tab.
3. Select a profile then perform one of the following.
   - To modify the settings or rules, either double-click the profile or click the **Edit Profile** icon.
   - To add assets to the profile, click the **Details** icon and switch to the **Assets** tab of the details window.

- To add accounts to the profile, click the **Details** icon and switch to the **Accounts** tab of the details window.
- To add password sync groups, click the **Details** icon and switch to the **Password Sync Groups** tab of the details window.

  On the **Password Sync Groups** tab, add or update a password sync group governed by the partition profile change schedule. For more information, see Password sync groups on page 432.

  - Click **Add** to create a new password sync group associated with the partition profile and assign accounts. The **Password Sync Group** dialog displays. For more information, see Adding a password sync group.
  - Click **Delete Selected** to remove the selected password sync group.
  - Click **Refresh** to refresh the selected password sync group.
  - Click **Edit** to modify the selected sync group and account assignments. The **Password Sync Group** dialog displays. For more information, see Modifying a password sync group on page 434.
  - Click **Change Sync Group Password** to reset the selected sync group password. When selected, accounts in the sync group re-sync with the new sync group password.

Related Topics

Assigning assets or accounts to a profile

Creating a profile

Setting a default partition

Each Asset Administrator can set a unique default partition and partition profile so that all new assets that administrator adds are automatically assigned to the default partition and default partition profile. For more information, see Setting a default partition profile on page 305.

To set the default partition

1. Navigate to **Administrative Tools** | **Partitions**.
2. In **Partitions**, right-click a partition and choose **Set as Default** from the context menu.

   -OR-
3. Select a partition and click **Set as Default** from the toolbar.

Setting a default partition profile

When you create a new partition, Safeguard for Privileged Passwords creates a corresponding default profile with default schedules and rules. Each Asset Administrator can set a unique default partition and partition profile. Once you set a default profile, all new assets and accounts you add are automatically assigned to that profile.

Safeguard for Privileged Passwords sets the default schedules to "Never" verify or reset passwords. To change the settings, see Modifying a profile.

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 partition profiles on page 293.

To set another profile as the default

1. Navigate to **Administrative Tools** | **Partitions**.
2. In **Partitions**, select a partition from the object list and open the **Profiles** tab.
3. Select a profile that is not the current default and click **Set as Default** from the details toolbar or context menu.

Assigning assets or accounts to a profile

This topic explains how to assign an asset or an account to a profile. You can only add assets and accounts to a profile that are assigned to the scope of the partition.

You can also configure Safeguard for Privileged Passwords to run automatic Asset Discovery or Account Discovery jobs. For more information, see Discovery on page 233.

Only associate accounts to a profile that you want Safeguard for Privileged Passwords to manage. For example, a directory can be added to any partition as an asset and any profile can be assigned. If directory user accounts are associated with a partition profile, Safeguard for Privileged Passwords will automatically change the user passwords according to the change password schedule in the profile. Depending on the settings, this could prevent a directory user from logging in to Safeguard for Privileged Passwords.

To add assets or accounts to a partition profile

1. Navigate to **Administrative Tools** | **Partitions**.
2. Select a partition from the object list and clickn the **Profiles** tab.
3. Select a profile and click the **Details** icon.
4. To add an asset to the selected partition profile, switch to the **Assets** tab of the partition profile's details window.
   a. Click **+ Add Asset**.
   b. On the **Asset** dialog, select the assets to be added.
   c. Click **OK**.

5. To add an account to the selected partition profile, switch to the **Accounts** tab of the partition profile's details window.
    a. Click **+ Add Account**.
    b. On the **Account** dialog, select the accounts to be added.
    c. Click **OK**.

If you do not see the account you are looking for, it might be assigned to a different partition. If you have have Asset Administrator permissions to create assets and accounts, you can click **+ Create New** to add an account. For more information, see Adding an account.

Related Topics

Assigning a profile to an asset

Setting a default partition profile

Modifying a partition

To modify a partition

1. Navigate to **Administrative Tools** | **Partitions**.
2. In **Partitions**, select a partition from the object list.
3. Select the view of the partition's information you want to modify (**General**, **Assets**, **Accounts**, **Profiles** or **SSH Key Profiles**).

    For example:

    - To change a partition's name or description, or delegate partition management to a user, click the **Edit** icon.

      NOTE: You can also double-click a partition name to open the **General** settings edit window.
    - To assign assets to the partition, open the **Assets** tab.

      NOTE: You can multi-select items to assign more than one asset to a partition.
    - To modify the password validation and reset settings, open the **Profiles** tab, select a profile, and click the **Edit** icon.
4. To set the default partition, select the partition, then click **Set as Default** from the toolbar or context menu.
5. To view or export the details of each operation that has affected the selected partition, open the **History** tab. For more information, see History tab on page 271.

Deleting a partition

When deleting a partition, you must designate another partition to transfers all assets and accounts. The partition 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 **Administrative Tools** | **Partitions**.
2. In **Partitions**, select a partition from the object list.
3. Click **Delete Selected**.
4. In the **Asset Partition** dialog, select the partition where assets and accounts are to be reassigned.
5. Click **OK** to reassign the assets and accounts and remove the selected partition.

20

Settings

(web client) Settings

In the web client, click the **Settings** menu on the left to go to the **Settings: Appliance** page.

The following **Settings** are available. See each section for a description of the functions available.

- **Appliance Information** (including shutting down and restarting the appliance): For more information, see Appliance Information on page 315.
- **Licensing**: For more information, see Licensing on page 321.
- **Networking**: For more information, see Networking on page 326.
- **Time**: For more information, see Time on page 330.

Additional information is available for **Networking** and **Time**. For more information, see How do I modify the appliance configuration settings on page 566.

(desktop client) Settings

Using the desktop client, the **Settings** page in the **Administrative Tools** is where you configure Safeguard for Privileged Passwords to run backups, install updates, manage clusters, manage certificates, enable event notifications, enable external integration, define profile configuration settings, define user password rules, define discovery rules, and run troubleshooting tools.

You must have administrator permissions to access the **Settings** page and the administrator permissions you have determine what you can do.

Use the **Search** control at the top of the **Settings** page to locate a particular setting. For example, if you type **password** and press the **Enter** key, a list of all the password settings appears; select an entry from this list to display the selected settings page.

The following **Settings** are available. See each section for a description of the functions available.

- Access Request settings
- Appliance settings
- Asset Management settings

- Backup and Retention settings
- Certificate settings
- Cluster settings
- External Integration settings
- Messaging settings
- Profile settings
- Safeguard Access settings

Access Request settings

Use the Access Request settings to enable (or disable) access request and password management services and to define global reason codes that can be used when creating access request policies.

Navigate to **Administrative Tools** | **Settings** | **Access Request**.

Table 106: Access Request settings

Setting	Description
Enable or Disable Services (Access and management services) Toggle on Toggle off	Where you enable or disable the following Safeguard for Privileged Passwords services: • Session requests • Password requests • Check password management • Change password management
Reasons	Where you configure access request reason codes, which can then be used when creating access request policies.

Enable or Disable Services (Access and management services)

Safeguard for Privileged Passwords allows you to enable or disable access request and password management services. These settings control session and password release requests, manual account

password validation, and reset tasks, as well as the automatic profile check and change tasks in Partitions.

All services are enabled by default. The toggles appear blue with the switch to the right when a service is enabled, and gray with the switch to the left when a service is disabled.

These global settings are enabled by default. By default, these 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 the access request and password management services.

Navigate to **Administrative Tools** | **Settings** | **Access Request** | **Enable or Disable Services**.

Table 107: Enable or Disable Services settings

Setting	Description
Requests	
Toggle on or Toggle off	
Session Requests Enabled	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 Enabled** 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 Enabled	Password requests are enabled by default, indicating that authorized users can make password release requests Click the **Password Requests Enabled** 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.
Password Management	
Toggle on or Toggle off	
Check Password Management Enabled	Check password management is enabled by default, indicating that Safeguard for Privileged Passwords 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 Enabled** toggle to

Setting	Description
	disable the password validation service. NOTE: Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords allows all currently running tasks to complete; however, no new tasks will be allowed to start.
Change Password Management Enabled	Change password management is enabled by default, indicating that Safeguard for Privileged Passwords 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 Enabled** toggle to disable the password reset service. NOTE: Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords allows all currently running tasks to complete; however, no new tasks will be allowed to start.
Discovery Toggle on or Toggle off	
Asset Discovery Enabled	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 Enabled	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 Enabled	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 233.
Directory Toggle on or Toggle off	

Setting	Description
Directory Sync Enabled	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 Management tab (add asset) on page 195.
Sessions Module	
Toggle on or Toggle off	
Session Module Password Access Enabled	Session module password access is disabled by default. When the toggle is on, Safeguard for Privileged Passwords (SPP) can create an access request and check out a password from Safeguard for Privileged Sessions (SPS) on behalf of another user. When the toggle is switched off, this ability is revoked. This functionality supports Safeguard for Privileged Sessions (SPS) version 6.2.0 or later. For more information, see the *One Identity Safeguard for Privileged Sessions Administration Guide*: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Reasons

In an access request policy, a Security Policy Administrator can require that a requester provide a reason for requesting access to a password 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 **Administrative Tools** | **Settings** | **Access Request** | **Reasons**.
2. Click **+ Add Reason** to add a new reason.
3. In the **Reason** dialog, enter the following:
   a. **Name**: Enter a name for the reason.

      Limit: 50 characters

      Required

   b. **Description**: Enter a description for the reason.

Limit: 255 characters

Required

4. Click **Add Reason**.
5. To edit a reason, click ✎ **Edit Reason**.

   The **Reason** dialog appears allowing you to modify the name or description.
6. To delete a reason, click 🗑 **Delete Reason**.

   In the confirmation dialog, click **Yes**.

Related Topics

Creating an access request policy

Appliance settings

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

Safeguard for Privileged Passwords can be set up to use a virtual appliance. For more information, see Using the virtual appliance and web management console on page 55.

Navigate to **Administrative Tools** | **Settings** | **Appliance**.

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

Table 108: 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. This page also contains power controls to shut down or restart your appliance.
Network Diagnostics	Where you run diagnostic tests on your appliance.
Enable or Disable Services	Where you enable or disable the Application to Application functionality.
Factory Reset from the desktop client	Where you perform a factory reset to revert your appliance to its original state when it first came from the factory.
Licensing	Where you add or update a Safeguard for Privileged Passwords license.

Setting	Description
Lights Out Management (BMC)	Where you enable and disable lights out management, which allows you to remotely manage the power state and serial console to Safeguard for Privileged Passwords using the baseboard management controller (BMC).
Networking	Where you view and configure the primary network interface, and if applicable, the sessions network interface.
Operating system licensing	Where you configure the operating system for the virtual appliance.
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. NOTE: A replica in the cluster will always reference the primary appliance as its NTP server.
Updates	Where you upload and install an update file. For more information, see Updates on page 331.

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

Table 109: Additional troubleshooting tools

Tool	Description
Activity Center	View the details of specific events or user activity. For more information, see Activity Center on page 94.
LCD status messages	An 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 544.
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 549.

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.

Navigate to **Administrative Tools** | **Settings** | **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**:

- From the web client, click the **Settings** menu on the left to go to the **Settings: Appliance** page. Click **Appliance Information** .
- From the desktop client, navigate to **Administrative Tools** | **Settings** | **Appliance** | **Appliance Information**.

The following information displays.

Table 110: Appliance properties

Property	Description
Appliance Name	The name of the appliance. To modify this name, click **Edit**.
Host	The appliance network server IP address.
Client Version	(If applicable) The version of the Safeguard for Privileged Passwords desktop client application.
Appliance Version	The version of the Safeguard for Privileged Passwords Appliance.
Uptime	The amount of time (hours and minutes) the appliance has been running.

(web client) Power (shut down or restart)

Power

Use the **Settings: Appliance** page, **Power**, you can enter a **Reason** and click the button to shut down or restart your appliance.

- For more information on shutting down the appliance, see Shutting down the appliance on page 318.
- For more information on restarting the appliance, see Restarting the appliance on page 319.

(desktop client) Additional information and power down

In the desktop client, the view also contains two tabbed pages to display general information and performance data for the appliance.

Appliance: General tab properties

Disk displays the amount of used and free disk space.

Table 111: General tab: Appliance properties

Property	Description
Manufacturer	The system manufacturer.
Model	The system model.

Property	Description
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 Toggle on Toggle off	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**.

Power

Use the power controls to shut down or restart your appliance.

- For more information on shutting down the appliance, see Shutting down the appliance on page 318.
- For more information on restarting the appliance, see Restarting the appliance on page 319.

Appliance: Performance tab properties

Table 112: Performance tab: Performance properties

Property	Description
Processor	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.

Setting the appliance name

Safeguard for Privileged Passwords automatically assigns a name to the appliance; however, you can change the name from the desktop client, **Appliance Information** page.

To set the appliance name

1. From the desktop client, navigate to **Administrative Tools** | **Settings** | **Appliance** | **Appliance Information**.
2. Click **Edit** to enable the **Appliance Name** text box.
3. Enter a new appliance name and click **Save**.

Shutting down the appliance

You can shut down an appliance from the Windows desktop client, 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

1. Go to **Appliance Information**:
   - From the web client, click **Settings** on the left. The **Settings: Appliance** page displays. Click **Appliance Information** .
   - From the desktop client, navigate to **Administrative Tools** | **Settings** | **Appliance** | **Appliance Information**.
2. Type an explanation for shutting down the Safeguard for Privileged Passwords Appliance in the **Reason** box and click **Shut Down**.

   IMPORTANT: 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.
3. To confirm your action, enter the words **Shut Down** in the box and click **OK**.
4. The Safeguard for Privileged Passwords Appliance LCD screen displays `LCD service terminating`.

NOTE: You can also 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

Use the Power controls on the **Administrative Tools** view in the Windows desktop client to restart an appliance.

To restart the appliance

1. Go to **Appliance Information**:
   - From the web client, click **Settings** on the left. The **Settings: Appliance** page displays. Click **Appliance Information** .
   - From the desktop client, navigate to **Administrative Tools** | **Settings** | **Appliance** | **Appliance Information**.
2. Type an explanation for restarting the Safeguard for Privileged Passwords Appliance in the **Reason** box and click **Restart**.
3. To confirm your action, enter the word **Restart** in the box and click **OK**.
4. The 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 544.

Enable or Disable Services

The Appliance Administrator can enable or disable services using toggles. The toggle appears blue with the switch to the right (toggle on) when the service is enabled, and gray with the switch to the left when the service is disabled (toggle off).

Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Enable or Disable Services**.

- **Application to Application Enabled** toggle: Use this toggle to enable or disable Application to Application service. It is the responsibility of the Appliance Administrator to manage the Application to Application service. The Application to Application service is disabled by default. For more information, see Application to Application on page 382.
- **Audit Enabled** toggle: Use this toggle to send Safeguard for Privileged Passwords data to Safeguard for Privileged Sessions (SPS) to audit the Safeguard privileged management software suite. The feature is disabled by default.

  NOTE: This feature is not fully functional until a future release of Safeguard for Privileged Sessions is available.

Factory Reset from the desktop client

As an Appliance Administrator, you can use the Factory Reset feature to reset a Safeguard for Privileged Passwords Appliance to recover from major problems or to clear the data and configuration settings on 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. 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 68.

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 you are using version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, you appliance will reset down to 6.0 LTS and you will have to patch up to your current version. For more information, see Long Term Support (LTS) and Feature Releases on page 46.

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 68.

To perform a factory reset from the desktop client

1. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Factory Reset**.
2. Click **Factory Reset**.
3. In the Factory Reset confirmation dialog, enter the words **Factory Reset** and click **OK**.

   The appliance will go into Maintenance mode to revert the appliance. Once completed, you will be prompted to restart the desktop client. 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 68. In addition, when you log in to the appliance, you will be prompted to add your Safeguard for Privileged Passwords licenses.

Licensing

It is the responsibility of the Appliance Administrator to manage the Safeguard for Privileged Passwords licenses. For more information, see License: hardware, virtual, expiration on page 45.To avoid disruptions in the use of Safeguard for Privileged Passwords, 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 396.

To enter licensing information when you first log in

The first time you log in as the Appliance Administrator, you are prompted to add one or more licenses. The **Success** dialog displays when a 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 42.

To add new licenses from Settings

1. Go to **Licensing**:
   - (web client): Click **Settings** on the left. The **Settings: Appliance** page displays. Click **Licensing** .
   - (desktop client): Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Licensing**.
2. Click + to upload a new license file.
3. **Browse** to select the license file.

   Once you add a license, you will see the current license information and a link that allows you to update the license.

These tasks can also be performed from **Licensing**:

- To add another module license, click + **Add License** and complete the information.
- To delete a license, select the license, then click **Delete**.

(desktop client) To update a module license

1. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Licensing**.
2. Select **Update License** in the lower left corner of a module's licensing information pane.
3. **Browse** to select the license file. Select **Open**.

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.

It is the responsibility of the Appliance Administrator to 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, Safeguard for Privileged Passwords immediately resets the password to a random value and resets the network settings to default values.

IMPORTANT: This feature requires a LAN interface to be enabled and configured. 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

1. Access Lights Out Management in one of two ways:
   - Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Lights Out Management (BMC)**.
   - Use the virtual appliance Support Kiosk, **Lights Out Managment (BMC)**. For more information, see Support Kiosk on page 58.
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. Click the **Set BMC Admin Password** button 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.

NOTE: Once Lights Out Management is enabled in Safeguard for Privileged Passwords, you can access the BMC via a web interface or by using SSH to connect to the IPMI port to remotely manage the power state and serial console to Safeguard for Privileged Passwords. The default user for accessing the BMC is ADMIN.

Network Diagnostics

Safeguard for Privileged Passwords 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.

Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Network Diagnostics**.

Table 113: Appliance Tests

Test	Description
Ping	To verify network connectivity and response time between the appliance to the specified host.
NS Lookup	To obtain DNS details of the specified host in relation to the appliance.
Trace Route	To obtain route information; traceroute determines the paths packets take from one IP address to another.
Telnet	To test TCP/IP connectivity between the appliance and specified host.
Show Routes	To retrieve routing table information.

Related Topics

Troubleshooting

Frequently asked questions

Ping

Use the ping test to verify network connectivity and response time between the Safeguard for Privileged Passwords Appliance and the specified host.

Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Diagnostics**.

Table 114: Ping diagnostic test settings

Property	Description
Ping through	Select the network interface to issue the diagnostic command: • **Network (X0)**: To ping the primary interface.
IP or Hostname	Enter the remote host's IP address or Hostname.
Ping	Click **Ping** to run the test. The test results display in the **Output** window.
More Settings	Select **More Settings** to configure these additional (optional) options: • Resolve IP addresses to hostnames • Number of echo requests to send • Send buffer size • Set 'don't fragment' flag in packet (IPv4 only) • Time to live • Type of serve • Record route for count hops (IPv4 only) • Time stamp for count hops (IPv4 only) • Timeout in milliseconds to wait for each reply

NS Lookup

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

Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Diagnostics**.

Table 115: NS Lookup diagnostic test settings

Property	Description
Network Interface	Select the network interface to issue the diagnostic command: • **Network (X0)**: To query at the primary interface.
IP or Hostname	Enter the remote host's IP address or Hostname.
Record Type	Select the type of DNS record to be queried.
Lookup	Click **Lookup** to run the test. The test results display in the **Output** window.

Trace Route

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

Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Diagnostics**.

Table 116: Trace Route diagnostic test settings

Property	Description
Trace route through	Select the network interface to issue the diagnostic command: • **Network (X0)**: To test the primary interface.
IP or Hostname	Enter the remote host's IP address or Hostname.
Trace	Click **Trace** to run the test. The test results display in the **Output** window.
More Settings	Select **More Settings** to configure these additional (optional) options: • Resolve IP addresses to hostname • Maximize number of hops to search for target • Timeout in milliseconds to wait for each reply

Telnet

Use telnet to test TCP/IP connectivity between the Safeguard for Privileged Passwords Appliance and the specified host.

Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Diagnostics**.

Table 117: Telnet diagnostic test settings

Property	Description
Connect through	Select the network interface to issue the diagnostic command: • **Network (X0)**: Select to test the primary interface.
IP or Hostname	Enter the remote host's IP address or Hostname.
Port	Enter the port number on a target host.
Connect	Click **Connect** to run the test. The test results display in the **Output** window.
More Settings	Select **More Settings** to configure this additional (optional) option:

Property	Description
	• Connection Timeout

Show Routes

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

Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Diagnostics**.

Table 118: Show Routes diagnostic test settings

Property	Description
Show Routes through	Select the network interface to issue the diagnostic command: • **Network (X0)**: To retrieve routing tables for the primary interface.
Show Routes	Click **Show Routes** 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.

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.

(web client) To modify the networking configuration settings

1. Click **Settings** on the left. The **Settings: Appliance** page displays.
2. Click **Networking** to configure the appliance.
3. Continue to the Network settings

(desktop client) To modify the networking configuration settings

1. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Networking**.
2. Click the ✎ **Edit** icon next to the Network Interface or Proxy Server heading to edit or configure the network properties.
3. Network settings

Network settings

Complete the network settings. For more information, see Modifying the IP address on page 328.

Network Interface X0 (primary interface)

Table 119: Network Interface X0 properties

Property	Description
MAC Address	The media access control address (MAC address), a unique identifier assigned to the network interface for communications
IP Address	The IPv4 address of the network interface
Netmask	The IPv4 network mask
Default Gateway	The IPv4 default gateway
IPv6 Address	The IPv6 address of the network interface
IPv6 Prefix Length	The IPv6 subnet prefix length
IPv6 Gateway	The IPv6 default gateway
DNS Servers	The IP address for the primary DNS servers
DNS Suffixes	The network suffixes for the DNS servers NOTE: You can modify the network suffixes for the DNS servers by clicking the ✎**Edit** icon next to the Network Interface X0 heading.

Proxy Server X0

The **Proxy Server X0** settings must be configured if your company policies do not allow devices to connect directly to the web. Once configured, Safeguard for Privileged Passwords uses the configured proxy server for outbound web requests to external integrated services, such as Starling.

NOTE: Only HTTP web proxy is supported.

Table 120: Proxy Server X0 properties

Property	Description
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. Value: Integer from 1 to 65535. NOTE: 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. NOTE: 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. NOTE: The username and password are only required if your proxy server requires them to be specified.

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 Safeguard for Privileged Passwords2.4 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. The desktop client will give guidance on screen as you wait for the changes to be completed.
5. 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 with the desktop client.
6. Repeat step 3, 4, and 5 for the other replicas.
7. Once the replicas are changed, proceed with the Primary.

Safeguard for Privileged Sessions (SPS) IP address change

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

1. Use the following information in the SPS documentation to understand SPS cluster roles, settings, and IP address updating.
    - Cluster roles: Assigning roles to nodes
    - Network settings: Setting SPS 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 join 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 SPS Managed Nodes
    - Managing a High Availability One Identity Safeguard for Privileged Sessions (SPS) cluster: Setting up SPS so, to handle nodes if the primary node stops functioning
2. If the IP address is changed, you must rejoin the cluster. For more information, see Joining SPS to SPP.
3. Once the SPS IP addresses are successfully changed, you will need to delete the session connection in the SPP settings and rejoin the SPS cluster master to the SPP primary. For more information, see SPP and SPS sessions appliance join guidance on page 592.

Operating system licensing

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 **Administrative Tools** | **Settings** | **Appliance** | **Operating System Licensing**. Click **Refresh** anytime to refresh the settings.
2. The display shows if **Windows is licensed with** KMS or licensed with a product key. Click **Details** to see additional information.
3. Click **Edit** to change the operating system license and select one of the following options.
    - **License automatically with KMS**: If you select this option, Safeguard will use DNS to locate the KMS server automatically.
    - **Specify a KMS server**: If KMS is not registered with DNS, enter the network IP address of your KMS server.
    - **Specify a license 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.

4. Click **OK**.

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.

NOTES: 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 549.

Virtual appliance support bundles are generate from the web management console. For more information, see Support Kiosk on page 58..

To create a support bundle

1. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Support Bundle**.
2. Click **Generate Support Bundle**.
3. Browse to select a location to save the support bundle .zip file and click **Save**.
4. Send the support bundle to One Identity Support. For more information, see About us on page 616.

Related Topics

Troubleshooting

Frequently asked questions

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.

It is the responsibility of the Appliance Administrator to manage the appliance time.

NOTE: A warning appears 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.

NOTE:**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.

To enable Network Time Protocol (NTP) and set the primary and secondary NTP servers

1. Go to **Time**:
   - In the web client, click **Settings** on the left. The **Settings: Appliance** page displays. Click **Time** .
   - In the desktop client, navigate to **Administrative Tools** | **Settings** | **Appliance** | **Time**.
2. Select the **Enable Network Time Protocol (NTP)** check box to enable NTP.
3. 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.
4. Click **OK** or **Save** to save your selections.

   When NTP is enabled, the following information about the NTP client status is displayed:
   - Last Sync Time
   - Leap Indicator
   - Poll Interval
   - Precision
   - Reference ID
   - Root Delay
   - Root Dispersion
   - Source
   - Stratum

   NOTE: Select **Show Last Sync Details** and **Hide Details** to display more or less information.

Related Topics

How do I set the appliance system time

Updates

It is the responsibility of the Appliance Administrator to update or upgrade 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.

Clustered environment

Apply the patch so all appliances in the cluster are on the same version. The procedure for patching cluster members depends on the Safeguard for Privileged Passwords version you are currently running.

- If you are running Safeguard for Privileged Passwords 2.0.1.x or earlier, you must unjoin replica appliances, install the patch on each appliance, and then enroll the replica appliances to rebuild your cluster. For more information, see Patching cluster members in the *Safeguard for Privileged Passwords 2.0 Administration Guide*.
- If you are running Safeguard for Privileged Passwords 2.1.x or 2.2.x, you can use the enhanced cluster patching feature where unjoining replica appliances is no longer required. For more information, see Patching cluster members on page 493.

To install an update file

1. Back up your system before you install an update file. For more information, see Backup and restore on page 348.
2. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Updates**. The current **Appliance Version**, **Client Version**, and **OS Version** display.
3. Click **Upload a File** and browse to select an update file.

   NOTE: When you select a file, Safeguard for Privileged Passwords uploads it to the server, but does not install it.
4. Once the file has successfully uploaded, click one of the following:
   - **Install Now** to install the update file.

     NOTE: Once you install an update file, you cannot uninstall it.
   - **Remove** to delete the file from the server without installing it.

   The **Updates** pane shows the upgrade progress and when the appliance has been successfully upgraded.

Asset Management settings

Use the Asset Management settings to define and manage dynamic tags for assets and asset accounts which include directory accounts. Asset Management settings allow you to add a custom platform.

Navigate to **Administrative Tools** | **Settings** | **Asset Management**.

Table 121: Asset Management settings

Setting	Description
Custom platforms	Where you add a custom platform
Tags	Where you view and manage dynamic tags for assets and asset accounts

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.

Create and manage custom platforms in **Administrative Tools** | **Settings** | **Asset Management** | **Custom Platforms**.

The **Custom Platform** pane displays the following.

Table 122: Custom platform: Properties

Property	Description
Name	The name of the platform type which may be a product name.
Version	The version of the target platform to use as an identifier.
Architecture	The CPU architecture to use as an identifier. If not applicable, use **Any**.
Platform Script	The name of the custom platform script file displays once selected.
Allow Sessions Requests	If selected, session access requests are allowed.

Use the following toolbar buttons to manage the custom platform settings.

Table 123: Custom Platform: Toolbar

Option	Description
Add	Add a custom platform. For more information, see Adding a custom platform.
Delete Selected	Remove the selected custom platform. **CAUTION: If the custom platform is associated with an asset, deleting the custom platform may halt password 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.**
Refresh	Update the list of custom platforms.
View	View the custom platform script parameters including: • **Supported operations**, for example Suspend and

Option	Description
	Restore Accounts, Check System, Check Password, Change Password • Details including **Name**, **Task**, **Type**, **Default**, and **Description**
Download Selected Script	Download the selected custom platform JSON script.

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 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. Safeguard for Privileged Passwords 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). Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords handles custom platforms. The custom platform script must be available for uploading. For more information, see Creating a custom platform script on page 334.

To add a custom platform

1. Have the custom platform script file available to upload.
2. Navigate to **Administrative Tools** | **Settings** | **Asset Management** | **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. **Version**: Enter the version of the target platform to use as an identifier.
   c. **Architecture**: Enter the CPU architecture to use as an identifier. If not applicable, use **Any**.
   d. **Platform Script**: Click **Browse**. Navigate to and select the script file. Click **Open**. The selected custom platform script file displays.
   e. 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 .`

Tags

Asset Administrators can define rules that will dynamically add tags to assets and asset accounts so that they can be easily identified and added to dynamic groups. Use the **Administrative Tools** | **Settings** | **Asset Management** | **Tags** pane to create and manage dynamic 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** pane 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 124: Tags: Properties

Property	Description
Name	The name assigned to the tag when it was created.
Asset Partition	The asset partition to which the tag belongs.
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 or asset account rule.
Description	Information about the tag.

Use these toolbar buttons to manage tags.

Table 125: Tags: Toolbar

Option	Description
New	Add a dynamic tag. For more information, see Adding a tag for dynamic tagging of assets or asset accounts on page 337.
Delete	Remove the selected tag. For more information, see Deleting an asset or asset account tag on page 341.
Refresh	Update the list of tags.
Edit	Modify the selected tag. For more information, see Modifying an asset or asset account tag on page 341. 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 342. 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 342.
Search	Search for a specific tag or set of tags in this list.

Related Topics

When does the rules engine run for dynamic grouping and tagging

Adding a tag for dynamic tagging of assets or asset accounts

Use the **+ New** button on the **Tags** pane in the **Asset Management** settings page to add a dynamic tag for an asset or asset account.

To add an asset or asset account dynamic tag

1. Navigate to **Administrative Tools** | **Settings** | **Asset Management** | **Tags**.
2. Click the **+ New** toolbar button.

   The **Tag** dialog displays.
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 **Account Rules** tab, enter the conditions for an account rule.
   - **Include an account 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 126: 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: • **Name** (Default) • **Description** • **Platform** • **Disabled** • **Tag** • **Service Account**

Property	Description
	• **Partition Name** • **Asset Name** • **Asset Tag** • **Domain Name** • **NETBIOS Name** • **Distinguished Name** (You cannot do a one level search with this attribute.) • **SID** • **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 • 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.

Property	Description
	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 **Asset Rules** tab, enter the conditions for an asset rule.
   - **Don't include an asset rule for this tag**: Select this check box if you do not want to include an asset rule. Selecting this check box disabled the rule editor controls on this page. Proceed to the next tab.
   - **Rule editor**: Use the rule editor to define conditions for tagging assets.

Table 127: 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: • **Name** (default) • **Description** • **Platform** • **Disabled** • **Tag** • **Discovery Job Name** • **Partition Name** • **Profile**

Property	Description
	• **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.) • **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

Property	Description
	search criteria.
Preview	Click **Preview** to run the query in order to review the results of the query before adding the dynamic tag.

6. On the **Summary** tab, review your selections.
   - **Account Rules**: Open the **Account Rules** tab to review the conditions for an asset account rule.
   - **Asset Rules**: Open the **Asset Rules** tab to review the conditions for an asset rule.
7. Click **Add** to create the tag, 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 **Administrative Tools** | **Settings** | **Asset Management** | **Tags**.
2. Select the tag to be deleted.
3. Click the 🗑 toolbar button.
4. On the **Remove Selected** 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, enter **Force Delete** and click **OK**.

Modifying an asset or asset account tag

Use the ✎ **Edit** 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 **Edit** 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 342.

To modify an asset or asset account tag

1. Navigate to **Administrative Tools** | **Settings** | **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 dynamic tagging of assets or asset accounts on page 337.

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 **Edit** 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 **Administrative Tools** | **Settings** | **Asset Management** | **Tags**.
2. Click the toolbar button. The **Copy to** 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.

   If you have Asset Administrator permissions, you can create a new partition by clicking **+ Create New**. For more information, see Adding a partition on page 300.
4. Click **OK**. 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 **Administrative Tools** | **Settings** | **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.
   - **Asset**: The name of the asset.
   - **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 **Close** to close the dialog and return to the **Tags** pane.

Backup and Retention settings

Use the Backup and Retention settings to manage your Safeguard for Privileged Passwords backups and archive servers.

It is the responsibility of the Appliance Administrator to configure the Safeguard for Privileged Passwords backup and retention settings.

To ensure the security of the hardware appliance, 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.

Navigate to **Administrative Tools** | **Settings** | **Backup and Retention**.

Table 128: Backup and Retention settings

Setting	Description
Archive servers	Where you add and manage archive servers for storing backup files and session recordings
Audit Log Management	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 Safeguard for Privileged Passwords to store on the appliance

About backups

Safeguard for Privileged Passwords backs up the following:

- All settings, except:
  - Appliance IP address
  - Network Time Protocol (NTP) configurations
  - Domain Name System (DNS) configuration
- Transaction history
- All information about Safeguard for Privileged Passwords objects:

- Accounts
- Account groups
- Assets
- Asset groups
- Entitlements
- Partitions
- Users
- User groups

Safeguard for Privileged Passwords encrypts and signs the data before it makes it available for downloading to an off-appliance storage. Only a genuine Safeguard for Privileged Passwords Appliance can decrypt the backup, and then only when it is on the appliance. This means that if a backup has been downloaded from an appliance for off-appliance storage, you must first upload it to an appliance, which will verify the signature, ensuring that it is an authentic backup for Safeguard for Privileged Passwords.

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.

Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Archive Servers**. The **Archive Servers** page displays the following information about previously configured archive servers.

Table 129: Archive Servers: Properties

Property	Description
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.
Description	Information about the archive server.

Use these toolbar buttons to manage archive server configurations.

Table 130: Archive Servers: Toolbar

Option	Description
Add Archive Server	Add an archive server. For more information, see Adding an archive server on page 345.
Delete Selected	Remove the selected archive server configuration.
Refresh	Update the list of archive server configurations.
Edit	Modify the selected archive server configuration.

You can store backup files on an external archive server. For more information, see Archive backup on page 354.

You can configure an automatic backup schedule and specify which archive server will be used to automatically archive after the scheduled backup. For more information, see Backup settings on page 350.

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. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Archive Servers**.
2. Click **Add Archive Server** and provide the following.
   - **Name**: Enter the display name for the archive server. Limit: 100 characters.
   - **Description**: Enter information about the archive server. Limit: 255 characters.
   - **Network Address**: Enter a network DNS name or the IP address used to connect to the server over the network. Limit: 255 characters.
   - **Storage Path**: Enter the file path where you want to store backup files on the archive server. Limit: 255 characters.
   - **Archive Method**: Choose a transfer protocol type:
     - **CIFS**: Common Internet File System
     - **SCP**: Secure Copy Protocol
     - **SFTP**: Secure File Transfer Program
   - **Port**: The port used by SSH to log in to the managed system. Not applicable for CIFS archive mode.

- **Authentication Type**: Select the type of authentication to be used to access the archive server (not applicable for CIFS archive mode.):
  - Password (default)
  - Directory Account
  - SSH
- **SSH Key Generation and Deployment Settings**: If **SSH** is selected as the authentication type, select one of the following settings:
  - Automatically Generate the SSH Key
  - Install and Use SSH Key from Safeguard for Privileged Passwords
  - Optionally, select **Manually Deploy the SSH key** check box. **Browse** to select the SSH key to be used.
- **Account Name**: If **Password** or **SSH** is selected as the authentication type, enter the service account name.
- **Password**: If **Password** or **SSH** is selected as the authentication type, enter the service account password.
- **Service Account**: if **Directory Account** is selected as the authentication type, click **Select Account** to chose the service account is be used to access the archive server.
- **Auto Accept SSH Host Key**: Select this check box to have Safeguard for Privileged Passwords automatically accept the SSH host key when it creates the archive server.
- **Test Connection**: Click this button to verify that the appliance can communicate with this archive server. For more information, see About Test Connection on page 202.

3. 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 354

Audit Log Management

Safeguard for Privileged Passwords allows you to define and schedule an audit log management task to purge audit logs from the Safeguard for Privileged Passwords Appliance and archive older audit logs 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.

> **CAUTION: The initial and subsequent archiving and purging of audit logs can take hours. The cluster is locked during the process. Carefully schedule and monitor this process.**

To define and schedule when to perform an audit log archival task:

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Audit Log Management**.
2. 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.

     - **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 **-** delete 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 AM**
     - **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 that 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 20:00:00 PM** and **Repeat 2**.

- **Time Zone**: Select the time zone.

3. Select an approach:
   a. Archive and delete logs:
      i. For **Archive and delete audit logs older than __ days**, enter the number of days that should pass before audit logs are archived to an archive server and deleted off the appliance.
      ii. Select **Send to archive server** to store the audit logs externally from the appliance during a scheduled backup or when manually running a backup.

      > NOTE: This option is only available if you have configured an archive server. For more information, see Adding an archive server on page 345.

      iii. Click **Test** to test the connection to the archive server.
   b. To delete audit logs from the appliance and not back them up on an archive server, enter the days in **Delete audit logs older than __ days**.
4. Click **OK**.

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 backup files, use **Delete** to remove them from the desktop client application. You can set the maximum number of backup files you want Safeguard for Privileged Passwords to retain on the appliance in Backup and Retention settings.

Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore**.

The **Safeguard for Privileged Passwords Backup and Restore** page lists this information for the backups that are currently in the database.

Table 131: Safeguard for Privileged Passwords Backup and Restore: Properties

Property	Description
Date	The date of the backup

Property	Description
Time	The time 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 Safeguard for Privileged Passwords Appliance
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

Use these toolbar buttons to manage Safeguard for Privileged Passwords backups

Table 132: Safeguard for Privileged Passwords 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 350.
Delete	Remove the selected backup file from the **Backups** page and the Safeguard for Privileged Passwords database.
Refresh	Update the list of backup files on the **Backups** page.
Settings	Where you configure an automatic backup schedule. For more information, see Backup settings on page 350.
Download	Save the selected backup file in a location on your appliance. For more information, see Download on page 352.
Upload	Retrieve a backup file from a file location and add it to the **Backups** page list. For more information, see Upload on page 352.
Restore	Overwrite the current data and restore Safeguard for Privileged Passwords to the selected backup. For more information, see Restore on page 353.
Archive	Store a backup file on an external archive server. For more information, see Archive backup on page 354.

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 350.

To create a new backup

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore**.
2. Click **+ Run Now**.

   Safeguard for Privileged Passwords makes a copy of the current database.

CAUTION: If you restore a backup that is older than the Maximum Password Age set in the 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: Safeguard for Privileged Passwords can not restore any access request workflow events in process at the time of a backup.

Backup settings

Settings is where you 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), Safeguard for Privileged Passwords will not execute another backup 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, Safeguard for Privileged Passwords will not run the backup until tomorrow.

The backup schedule window end time must be after the start time.

To schedule backups

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore**.
2. Click **Settings**.
3. In the **Backup Settings** dialog, specify the backup schedule. Select **Backup Every** to run the job along per the run details you enter. (If you deselect **Backup Every**, the 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.

  - **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 **-** delete 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 AM**
  - **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 that 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 20:00:00 PM** and **Repeat 2**.

- **Time Zone**: Select the time zone.

4. Select **Send to archive server** to store the backup files externally from the appliance during a scheduled backup or when manually running a backup.

   NOTE: This option is only available if you have configured an archive server. For more information, see Adding an archive server on page 345.

You configure the maximum number of backup files you want Safeguard for Privileged Passwords to store on the appliance on the Backup retention page.

Download

Safeguard for Privileged Passwords allows you to save a selected backup file in a location on your computer.

To download the backup file

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore**.
2. Select a backup file and click **Download**.
3. Browse to select a location of your choice.
4. Give the file a name and click **OK**.

NOTE: Safeguard for Privileged Passwords copies the backup file; it does not remove the backup from the list displayed on the Backup and Restore page.

Upload

Safeguard for Privileged Passwords allows you to retrieve a backup file from a file location and add it to the **Safeguard for Privileged Passwords Backup and Restore** page list on the appliance.

To upload a backup file

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore**.
2. Click **Upload**.
3. Browse to select a backup file and click **Open**.

Restore

Safeguard for Privileged Passwords allows you to restore the data on your appliance with data from a selected backup. Safeguard for Privileged Passwords does not restore the appliance IP address, NTP settings, or the DNS settings. To verify that these settings are correct after a restore, go to **Settings** | **Appliance Information**.

IMPORTANT: For on-prem VM (Hyper-V or VMware) only: If you upgrade from 2.x to 6.0 then restore a backup taken prior to 6.0, you will need to reassign session connections. See KB Article xxxx for resolution steps.

CAUTION: If you restore a backup that is older than the Maximum Password Age set in the 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. 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 552.

Version considerations when restoring a backup

An Appliance Administrator can restore backups as far back as Safeguard for Privileged Passwords version 2.2.0.6958. Only the data is restored; the running version is not changed.

If the administrator attempts to restore a version earlier than 2.2.0.6958, a message like the following displays: `Restore failed because the backup version '[version]' is older than the minimum supported version '2.2.0.6958' for restore.`

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 Safeguard for Privileged Passwords appliance from a selected backup

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore**.
2. Select a backup. If the backup file is not listed, you can Upload it first.
3. Click **Restore**.
4. When the **Restore** dialog diplays, enter the word **Restore** in the box and click **OK**.

   Safeguard for Privileged Passwords automatically restarts the appliance, if necessary.
5. 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

354.

- 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 management and discovery tasks will fail. For more information, see Managed networks on page 369.

6. Once the appliance is fully operational, it asks you to restart the Windows desktop 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

Safeguard for Privileged Passwords allows you to store backup files on an external archive server.

To archive a backup file

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard Backup and Restore**.
2. Select the backup to be archived.
3. Click **Archive** and select **Archive Backup**.
4. In the **Archive Servers** selection dialog, choose an archive server.

   NOTE: You can add an archive server from the **Archive Servers** selection dialog by clicking the **Add Archive Server** toolbar button.

Safeguard for Privileged Passwords copies the backup file to the archive server.

Backup retention

It is the responsibility of the Appliance Administrator to configure the maximum number of backup files you want Safeguard for Privileged Passwords to store on the appliance.

To configure the appliance backup retention settings

1. Navigate to **Administrative Tools** | **Settings** | **Backup and Retention** | **Safeguard for Privileged Passwords Backup Retention**.
2. Select the **Enable Backup Retention** check box.
3. Enter the maximum number of backup files you want to store on the appliance.
4. Click **OK**.

Once Safeguard for Privileged Passwords saves the maximum number of backup files, next time it performs a backup, it deletes the backup file with the oldest date.

Certificate settings

Use the Certificate settings to manage the certificates used to secure 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 Safeguard for Privileged Passwords.

It is the responsibility of the Appliance Administrator to manage the certificates used by Safeguard for Privileged Passwords.

Navigate to **Administrative Tools** | **Settings** | **Certificates**.

Table 133: 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.
Certificate Signing Request	Where you can view and manage certificate signing requests (CSRs)
SSL Certificates	Where you manage SSL certificates, including installing SSL certificates or creating CSRs to enroll a public SSL certificate.
Trusted Certificates	Where you add and manage certificates trusted by Safeguard for Privileged Passwords, for example your company's root Certificate Authority (CA) certificate.

About certificates

The certificate infrastructure in Safeguard for Privileged Passwords consists of the following.

Replaceable certificates

Safeguard for Privileged Passwords ships with the following default certificates which are meant to be replaced:

- A self-signed SSL certificate for HTTPS.

  The name of the SSL certificate matches the hostname of the Safeguard for Privileged Passwords Appliance and uses the appliance's default IP addresses as the Subject Alternative Name (SAN).
- A signing certificate used to validate that archived audit logs were created by and came from Safeguard for Privileged Passwords.

User-supplied certificates

Safeguard for Privileged Passwords allows you to specify the security certificates to be used. When replacing or adding certificates, keep the following considerations in mind:

- Safeguard for Privileged Passwords supports Certificate Signing Requests (CSRs) to enroll any type of certificate. CSRs use the Public-Key Cryptography Standard (PKCS) #10 format.
- For imports, Safeguard for Privileged Passwords must access the relevant network resources to validate the CRL end points specified in the signed CSR.
- For uploading certificates with private keys, Safeguard for Privileged Passwords supports .pfx (or .p12) files that follow the PKCS #12 standard.
- For SSL certificates, Safeguard for Privileged Passwords allows you to upload or use a CSR to enroll multiple certificates that can then be applied to different appliances.
- Safeguard for Privileged Passwords provides an SSL certificate store that allows you to assign any uploaded or enrolled SSL certificate to any appliance.
- Prior to adding an asset that uses SSL server certificate validation, you must add the server's signing authority certificate to the Trusted Certificates store in Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords (SPP) cluster.

Define an audit log signing certificate

You can have only one audit log signing certificate defined, which is used by all Safeguard for Privileged Passwords 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 signing certificate.

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 a Certificate Signing Request for audit logs. The administrator will have a copy of the public key which will be used to verify the validity of the archived audit logs.

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 Safeguard for Privileged Passwords cluster.

The certificate's public key and the certificate's issuer, must be available to validate the signed audit log.

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>`

Managing audit log signing certificates

Navigate to **Administrative Tools** | **Settings** | **Certificates** | **Audit Log Signing Certificate**. The following properties and controls are available to manage your audit log signing certificate.

Table 134: Audit Log Certificates: Properties

Properties/Controls	Description
Refresh	Click **Refresh** to update the certificate displayed on the **Audit Log Certificates** pane.

Properties/Controls	Description
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.
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)**
Use Default	Click **Use Default** to reset the certificate back to the default.

Installing an audit log signing certificate

It is recommended that you not use the default certificate provided with Safeguard for Privileged Passwords. Instead, replace it with another certificate with a private key.

To replace the default certificate with your own, the certificate must have the following:

- Enhanced Key Usage extension with the Server Authentication (1.3.6.1.5.5.7.3.1) OID value.
- Digital Signature key Usage extension with the Server Authentication (2.5.29.37.3) OID value.

For uploading certificates with private keys, Safeguard for Privileged Passwords supports .pfx (or .p12) files which follow the PKCS #12 standard.

To install an audit log signing certificate

1. Navigate to **Administrative Tools** | **Settings** | **Certificates** | **Audit Log Signing Certificate**.
2. Click the **Add Certificate** button for the sessions 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 (.pfx file) and click **OK**.
4. Once installed, this new certificate will replace the default certificate listed on the **Audit Log Signing Certificates** pane.

Creating a Certificate Signing Request for audit logs

If you do not want to use a default sessions certificate provided with Safeguard for Privileged Passwords, you can enroll a certificate using a Certificate Signing Request (CSR) to replace the default certificate.

To create a CSR for an audit log signing certificate

1. Navigate to **Administrative Tools** | **Settings** | **Certificates** | **Audit Log Signing 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. Maximum length of 500 characters.

      NOTE: Click **Use Distinguished Name Creator** to create the distinguished name based on fully-qualified domain name, department, organization unit, locality, state/county/region, and country.

   b. **Alternate DNS Names**: Optionally, enter additional or alternate host names (such as, IP addresses, sites, or common names) that are to be protected by this certificate.

   c. **Key Size**: Select the bit length of the private key pair. The bit length determines the security level of the certificate. A higher bit length means stronger security.
      - 1024
      - 2048 (default)
      - 4096
4. Click **OK** to save your selections and enroll the certificate.

   Certificates enrolled via CSR are listed in the **Certificate Signing Request** pane.

Certificate Signing Request

Some certificates require a digital signature before a certification authority (CA) can process the certificate request. 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.

NOTE:Safeguard for Privileged Passwords supports the Public-Key Cryptography Standard (PKCS) #10 format for CSRs.

Navigate to **Administrative Tools** | **Settings** | **Certificates** | **Certificate Signing Request**. Certificates enrolled via a CSR appear on this pane including the following details.

Table 135: 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
Thumbprint	A unique hash value that identifies the certificate
Key Size	The bit length of the private key pair

Use these toolbar buttons to manage certificate signing requests.

Table 136: Certificate Signing Request: Toolbar

Option	Description
Delete Selected	Delete the selected CSR from Safeguard for Privileged Passwords.
Refresh	Update the list of CSRs.

SSL Certificates

Safeguard for Privileged Passwords 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.

Navigate to **Administrative Tools** | **Settings** | **Certificates** | **SSL Certificates**. The **SSL Certificates** pane displays the following information for the SSL certificates stored in the database.

Table 137: SSL Certificates: Properties

Property	Description
Appliances	Lists the name of the appliance to which the certificate is assigned.
Subject	The name of the subject (such as user, program, computer,

Property	Description
	service, or other entity) assigned to the certificate when it was requested.
Alternate DNS Names	Additional or alternate host names (such as IP addresses, sites, common names) that were specified when the certificate was requested. 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.
Thumbprint	A unique hash value that identifies the certificate.
Issued By	The name of the certificate authority (CA) that issued the certificate.

Use these toolbar buttons to manage SSL certificates.

Table 138: SSL Certificates: Toolbar

Option	Description
Add Certificate | Upload Certificate	Upload an SSL certificate. For more information, see Installing an SSL certificate on page 362.
Add Certificate | Create Certificate Signing Request (CSR)	Create a CSR to enroll a certificate. For more information, see Creating a Certificate Signing Request on page 362.
Assign Certificate to Appliance(s)	Assign the selected certificate to one or more appliances. For more information, see Assigning a certificate to appliances on page 363.
Unassign Certificate	Unassign the selected certificate from one or more appliances.
Delete Selected	Delete the selected certificate from Safeguard for Privileged Passwords.
Refresh	Update the list of SSL certificates available (uploaded to Safeguard for Privileged Passwords).

Installing an SSL certificate

To install an SSL certificate

1. Navigate to **Administrative Tools** | **Settings** | **Certificates** | **SSL Certificates**.
2. Click **+ Add Certificate** and select **Upload Certificate**.
3. **Browse** to select the certificate file.
4. After the certificate has been uploaded, assign the certificate to one or more appliances. For more information, see Assigning a certificate to appliances on page 363.

   You may also upload the certificate's root CA to the list of trusted certificates. For more information, see Trusted Certificates on page 363.

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 Safeguard for Privileged Passwords SSL Webserver Certificate. This way, no administrator will have access to the private SSL key that is used by Safeguard for Privileged Passwords and the traffic will be secure.

Creating a 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. Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords Appliances.

To create a CSR for SSL

1. Navigate to **Administrative Tools** | **Settings** | **Certificates** | **SSL 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. Maximum length of 500 characters.

      NOTE: Click **Use Distinguished Name Creator** to create the distinguished name based on fully-qualified domain name, department, organization unit, locality, state/county/region, and country.

b. **Alternate DNS Names**: Optionally, enter additional host names (such as, IP addresses, sites, common names) that are to be protected by this certificate.

c. **Key Size**: Select the bit length of the private key pair:

- 1024
- 2048 (default)
- 4096

NOTE: The bit length determines the security level of the SSL certificate. A higher bit length means stronger security.

4. Click **OK** to save your selections and enroll the certificate.

   Certificates enrolled via CSR are listed in the SSL Certificates pane and the Certificate Signing Request pane.

Assigning a certificate to appliances

Safeguard for Privileged Passwords 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. Navigate to **Administrative Tools** | **Settings** | **Certificates** | **SSL Certificates**.
2. Select a certificate from the grid and click the **Assign Certificate to Appliance(s)** toolbar button.
3. In the **Appliances** selection dialog, select one or more appliances and click **OK** to save your selection.

Trusted Certificates

It is the responsibility of the Appliance Administrator to add or remove trusted root certificates to the Safeguard for Privileged Passwords Appliance, if necessary, in order for the SSL certificate to resolve the chain of authority. When Safeguard for Privileged Passwords connects to an asset that has the **Verify SSL Certificate** option enabled, Safeguard for Privileged Passwords compares the signing authority of the certificate presented by the asset to the certificates in the trusted certificate store.

Navigate to **Administrative Tools** | **Settings** | **Certificates** | **Trusted Certificates**. The **Trusted Certificates** pane displays the following information for the user-supplied certificates added to the trusted certificate store.

Table 139: Trusted 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.
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.
Thumbprint	A unique hash value that identifies the certificate.
Issued By	The name of the certificate authority (CA) that issued the certificate.

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 Safeguard for Privileged Passwords.

To add a trusted certificate

1. Navigate to **Administrative Tools** | **Settings** | **Certificates** | **Trusted Certificates**.
2. Click + **Add Certificate** from the details toolbar.
3. Browse to select a certificate file (DER Encoded file: .cer or .der).
4. Click **Open** to add the selected certificate file to Safeguard for Privileged Passwords.

Removing a trusted certificate

To remove certificates from the appliance

1. Navigate to **Administrative Tools** | **Settings** | **Certificates** | **Trusted Certificates**.
2. Select a certificate.
3. Click 🗑 **Delete Selected** from the details toolbar.

   IMPORTANT: Safeguard for Privileged Passwords does not allow you to remove built-in certificate authorities.

Cluster settings

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 Safeguard for Privileged Passwords cluster, become familiar with the Disaster recovery and clusters chapter to understand:

- Primary and replica appliances
- Consensus
- Supported clusters in Safeguard for Privileged Passwords
- 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 497.

Navigate to **Administrative Tools** | **Settings** | **Cluster**.

Table 140: 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 486.
Session Appliances with SPS join	Where you view, edit, and delete join connections when a Safeguard for Privileged Sessions (SPS) cluster is joined to a Safeguard for Privileged Password (SPP) for session recording and auditing. For more information, see SPP and SPS sessions appliance join guidance on page 592.

Cluster Management

Navigate to **Administrative Tools** | **Settings** | **Cluster** | **Cluster Management**.

The **Cluster Management** page is divided into left and right panes. If you do not see the right pane, click an appliance node in the left pane.

The health indicators on the nodes indicate if cluster members are in an error, warning, locked, or healthy state.

- Cluster view pane: The left pane displays a graphical representation of the primary and replica appliances belonging to the cluster.
- Appliance details and cluster health pane: The right pane displays details about the appliance selected in the left pane. From this pane you can run maintenance and diagnostic tasks against the selected appliance.

Cluster Management toolbar

Use these toolbar buttons on the **Cluster Management** page to manage the members of a cluster.

Table 141: Cluster Management: Toolbar

Option	Description
Back	Return to the main Settings view.
Add Replica	Join an appliance to the primary appliance as a replica. For more information, see Enrolling replicas into a cluster on page 482.
Refresh	Update the list of appliances in a cluster.
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 497. **CAUTION: Resetting a cluster should be your last resort. It is recommended that you restore from a backup rather than reset a cluster.**
Enable Offline Workflow (appliance has lost consensus)	Manually place the 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 489.
Resume Online Operations (appliance is in Offline Workflow Mode)	Manually reintegrate the appliance with the cluster and merge audit logs. For more information, see To manually resume online operations on page 490.

Cluster view pane

Navigate to **Administrative Tools** | **Settings** | **Cluster** | **Cluster Management**.

Initially, the Cluster view pane (left pane) displays a single primary node for the appliance you are currently logged in to. As you join appliances to the cluster, replica nodes will be shown as being connected to the primary node.

The health indicators on the nodes and in the upper-right corner of this pane provide a quick view as to whether cluster members are in an error, warning, or healthy state.

A warning icon identifies a potential issue with the cluster. An error icon indicates a definite problem impacting the functionality of the cluster. A lock icon indicates the cluster is locked. Expand the **View More** section to see more details.

Clicking a member of the cluster in this pane displays details about the appliance and the health of the cluster member. For more information, see Appliance details and cluster health pane on page 367.

Appliance details and cluster health pane

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 on the Cluster settings screen.

Navigate to **Administrative Tools** | **Settings** | **Cluster** | **Cluster Management**. In the cluster view (left pane), click a member of the cluster to refresh the display of the right pane. From the right pane you can monitor the health of the selected appliance and perform operations against the appliance:

- **Unjoin**: Click **Unjoin** to remove a replica from the cluster. For more information, see Unjoining replicas from a cluster on page 483.
- **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 491.
- **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 492.

  CAUTION: Activating an appliance that is in Read-Only mode will take it out of the Read-only state and enable password check and change for managed accounts. Ensure that no other Safeguard for Privileged Passwords 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 information. For more information, see Appliance Information on page 315.
- Run diagnostic tests against the appliance. For more information, see Network Diagnostics on page 323.
- Perform a factory reset. For more information, see Factory Reset from the desktop client on page 320.
- View or edit networking settings. For more information, see Networking on page 326.
- Generate a support bundle. For more information, see Support bundle on page 330.
- View or edit time settings. For more information, see Time on page 330.

- **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**.

Below the toolbar, this pane displays the following information about the appliance selected in the cluster view.

Table 142: Appliance properties

Property	Description
Appliance name	The name of the appliance.
IP address	The IPv4 address (or IPv6 address) of the appliance configuration interface. NOTE: You can modify the appliance IP address. For more information, see How do I modify the appliance configuration settings on page 566.
Appliance type	Indicates either **Primary** or **Replica**.
Appliance state	Indicates the appliance state. For a list of available states, see Appliance states on page 502.
Disk Space	The amount of used and free disk space.

Click **View More** to show or hide this additional information.

Appliance

Property	Description
Serial Number	The serial number of the appliance
Uptime	The amount of time (days, hours, and minutes) the appliance has been running

Primary (displayed on replicas)

Property	Description
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.

Information

Property	Description
Last Health Check	Last date and time Safeguard for Privileged Passwords obtained the selected appliance's information
Version	The appliance version number
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.`

Managed networks

Managed networks are named lists of network segments serviced by a specific Safeguard for Privileged Passwords (SPP) or Safeguard for Privileged Sessions (SPS) appliance in a clustered environment. Managed networks are used for scheduling tasks, such as password 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.

An 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 joined SPS 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 SPS 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 (Administrative Tools | 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.**

Task delegation

A Safeguard for Privileged Passwords' cluster delegates platform management tasks (such as password check and password 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 (SPS) 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 SPS 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 SPS 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.

Precedence

The selection made on the **Entitlement** | **Access Request Policy** tab takes precedence over the selections on **Settings** | **Cluster** | **Managed Networks** page. If a **Managed Networks** rule includes nodes from different SPS clusters, SPP will only select the nodes from the same cluster that was assigned on the **Session Settings** page of the **Access Request Policy** tab.

Navigate to **Administrative Tools** | **Settings** | **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.

IMPORTANT: Discovery and password 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 and/or sessions or delete the managed network entry.

Table 143: Managed Networks: Properties

Property	Description
Name	The name assigned to the managed network when it was added to Safeguard for Privileged Passwords.
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 joined 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 SPS appliance host name followed by the IP address of the SPS 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.

Click a managed network row to bring up the **Managed Network** dialog where the properties are editable.

Table 144: Managed Networks: Editable Properties

Property	Description
Name	The name assigned to the managed network when it was added to Safeguard for Privileged Passwords.
Description	The descriptive text entered when defining the managed network.
Subnets	A list of subnets included in the managed network. Click **Add** to add a subnet. Click **Delete** to delete the selected subnet.
Passwords Managed By	The host name and IP address of the appliances and the MAC address assigned to manage the specified subnets. Click **Add** to make a selection. Click **Delete** to delete the selected host name and IP address.
Sessions Managed By	The host name and IP address of the cluster master for the managed nodes. Click **Add** to make a selection given this information: **Host Name**, **Network Address**, and cluster **Master or Replica**. Click **Delete** to delete the selected host name and IP address.

Use these toolbar buttons to define and maintain your managed networks.

Table 145: Managed Networks: Toolbar

Option	Description
New	Add a managed network. For more information, see Adding a managed network on page 373.
Delete Selected	Remove the selected managed network from Safeguard for Privileged Passwords. 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.

Option	Description
Resolve Network	Locate an IP address in a managed network's list of subnets. For more information, see Resolving IP address on page 374.

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. Navigate to **Administrative Tools** | **Settings** | **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 joined SPS 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 374.

   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 (SPS) 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. Navigate to **Administrative Tools** | **Settings** | **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. Navigate to **Administrative Tools** | **Settings** | **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.

For general information on Offline Workflow Mode, see About Offline Workflow Mode.

Navigate to **Administrative Tools** | **Settings** | **Cluster** | **Offline Workflow**. The **Offline Workflow** page displays the following information.

Table 146: 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 147: 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 376.

To configure automatic settings to control Offline Workflow Mode

1. Navigate to **Administrative Tools** | **Settings** | **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.
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 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 is restored.
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 five minutes or more.
6. Click **OK**.

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. Navigate to **Administrative Tools** | **Settings** | **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 366.

To manually Resume Online Operations

This option is only available when the appliance is in Offline Workflow Mode.

1. Navigate to **Administrative Tools** | **Settings** | **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, click **Restart Desktop Client**. 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 366.

Session Appliances with SPS join

The Asset Administrator can join a Safeguard for Privileged Sessions (SPS) cluster to a Safeguard for Privileged Password (SPP) cluster of one appliance or more for session recording and auditing. The actual join must be between the SPP primary and the SPS cluster master. This means that the Safeguard for Privileged Sessions (SPS) cluster is aware of each node in an SPP cluster and vice-versa.

Once joined, all sessions are initiated by the SPP appliance via an access request and managed by the SPS appliance and sessions are recorded via the Sessions Appliance.

NOTE: If you have a single node SPS 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 SPS appliance in the cluster that is capable of recording sessions. See the *SPS Administration Guide*, Managing Safeguard for Privileged Sessions (SPS) clusters.

Safeguard for Privileged Passwords join guidance

Before initiating the join, review the steps and considerations in the join guidance. For more information, see SPP and SPS sessions appliance join guidance on page 592.

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 an SPS 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 SPS 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 SPS 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 join

If you add another SPS cluster after the initial join, follow these standard operating procedures:

1. Add join connections. See Viewing, deleting, or editing join connections later in this topic.

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 on page 276.
3. Assign the managed networks. For more information, see Managed networks on page 369.

If the SPS Central Management node is down

SPP continues to launch sessions on the managed hosts when the SPS 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 SPS cluster topology. See the *Safeguard for Privileged Sessions Administration Guide*, Managing a High Availability One Identity Safeguard for Privileged Sessions (SPS) cluster.

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 from the desktop client, the connection information is soft deleted so that a rejoin of the same SPS appliance can reuse the same values. This approach of soft deleting and reusing the same connection values on a rejoin avoids "breaking" all of the Access Request Polices that referenced the previous session connection.

If the session connection is deleted, a caution displays when you navigate to **Administrative Tools** | **Entitlements** | **Access Request Policies** and go to the **Session Settings** tab. For more information, see Session Settings tab on page 285.

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 rejoin is not desired or retaining the previous session connection values is preventing an SPS appliance from joining or rejoining.

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>

See OneIdentity/safeguard-ps.

Hard delete 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 /v3/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 /v3/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.

Viewing, deleting, or editing join connections

Once the join is complete, navigate to **Administrative Tools** | **Settings** | **Cluster** | **Session Appliances** to view, delete, or edit join connections. The **Session Appliances** pane displays the following session details.

Table 148: Session Appliances: Properties

Property	Description
Host Name	The host name of the SPS appliance host cluster master.
Network Address	The network DNS name or IP address of the session connection.
Description	(optional) Descriptive text about the SPS session connection (for example, 20 on cluster - 172 primary node).
Connection User	The user name for Safeguard for Privileged Passwords (SPP). Do not include spaces in the user name.
Thumbprint	A unique hash value that identifies the certificate.
Managed Hosts	Other nodes in the SPS cluster identified by the

Property	Description
	managed host name and IP address. Hover over any ⚠ **Warning** icon to see if the **Managed Host** is **Unavailable** or **Unknown**.

Click a **Host Name** row to bring up the **Session Module Connection** dialog.

Table 149: Session Module Connection: Properties

Property	Description
Node ID	The name of the Safeguard for Privileged Sessions Appliance used to authenticate the joined SPS session connection.
Host Name	The host name of the SPS appliance host cluster master.
SPP Username	The user name for Safeguard for Privileged Passwords (SPP). Do not include spaces in the user name.
Description	(optional) Descriptive text about the SPS 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 (not IP address)	If checked, the connection string used to launch a session uses the host name of the SPS appliance rather than the IP address.

Use these toolbar buttons to manage sessions.

Table 150: Sessions Management: Toolbar

Option	Description
Delete Selected	Remove the selected joined SPS session connection. For details on soft versus hard deletes, see Connection deletion: soft delete versus hard delete earlier in this topic.
Edit	Modify the selected joined SPS session connection **Description** or **Network Address** on the **Session Module Connection** dialog.
Refresh	Update the list of joined SPS session connections.

Option	Description
Session Module Password Access Enabled Toggle on Toggle off	**CAUTION: This functionality supports the join with Safeguard for Privileged Sessions (SPS) version 6.2.0 or later. The toggle function is used to enable an SPS initiated session to get the session credentials from SPP. For information see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.**

External Integration settings

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.

However, it is the Security Policy Administrator's responsibility to configure the Approval Anywhere feature.

Navigate to **Administrative Tools** | **Settings** | **External Integration**.

Table 151: External Integration settings

Setting	Description
Application to Application	Where you configure application registrations to use the Application to Application service, which allows third-party applications to retrieve credentials from Safeguard for Privileged Passwords
Approval Anywhere	Where you define the Safeguard for Privileged Passwords users who are authorized to use Approval Anywhere to approve access requests
Email	Where you configure Safeguard for Privileged Passwords to automatically send email notifications when certain events occur
Identity and Authentication	Where you configure the identity providers and authentication providers to use when logging into Safeguard for Privileged Passwords
SNMP	Where you configure Safeguard for Privileged Passwords to send SNMP traps to your SNMP console when certain events occur

Setting	Description
Starling	Where you join Safeguard for Privileged Passwords to Starling to take advantage of other Starling services, such as Starling Two-Factor Authentication (2FA) and Starling Identity Analytics & Risk Intelligence
Syslog	Where you configure Safeguard for Privileged Passwords to send event notifications to a syslog server with details about the event
Ticketing systems	Where you configure Safeguard for Privileged Passwords to integrate with your company's external ticket system or track generic tickets and not integrate with an external ticketing system

Application to Application

In order for third-party applications to use the Application to Application service to integrate with the Safeguard for Privileged Passwords vault, you must first register the application in Safeguard for Privileged Passwords. This can be done using the **Administrative Tools** | **Settings** | **External Integration** | **Application to Application** pane described below. Once the application is registered, you can enable or disable the service. For more information, see Enable or Disable Services on page 319.

The **Application to Application** pane 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** pane displays the following details about application registrations.

Table 152: 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 Safeguard for Privileged Passwords 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

Property	Description
	registration is enabled again.
Description	Information about the application's registration.

Use these toolbar buttons to manage application registrations.

Table 153: Application to Application: Toolbar

Option	Description
Add	Add an application registration to Safeguard for Privileged Passwords. For more information, see Adding an application registration on page 386.
Delete Selected	Remove the selected application registration from Safeguard for Privileged Passwords. For more information, see Deleting an application registration on page 388.
Refresh	Update the list of application registrations.
Edit	Modify the selected application registration.
API Keys	Display the API keys that were generated for Access Request Broker or Credential Retrieval. An API key can then be copied and used in the third-party application to authenticate with Safeguard for Privileged Passwords. NOTE: For credential retrieval, the registration process generates an API key for each managed account. However, for access request broker, the registration process generates a single API key for all users or user groups that are added.

About Application to Application functionality

Using the Application to Application service, third-party applications can interact with Safeguard for Privileged Passwords in the following ways:

- Credential retrieval: A third-party application can retrieve a credential from the Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 486.

Credential retrieval

A credential retrieval request using the Application to Application service allows the third-party application to retrieve credentials from the Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords. 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords.

  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. An Appliance Administrator can use the desktop client or Safeguard for Privileged Passwords API to enable the service.

Using the desktop client:

1. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Enable or Disable Service**.
2. Click the **Application to Application Enabled** toggle to enable the service (toggle on).

Using the API, use the following URL:

```
https://appliance/service/appliance/v2/A2AService/Enable
```

In addition, you can check the current state of the service using this same desktop client page or using the following URL:

```
https://appliance/service/appliance/v2/A2AService/Status
```

Related Topics

Setting up Application to Application

Making a request using the Application to Application service

Setting up Application to Application

In order to use Application to Application integration with Safeguard for Privileged Passwords, you must perform the following tasks:

Step 1: Prepare third-party application for integration with Safeguard for Privileged Passwords.

Step 2: Appliance Administrator enables Application to Application service in Safeguard for Privileged Passwords.

Using the desktop client, navigate to **Administrative Tools** | **Settings** | **Appliance** | **Enable or Disable Service** and click the **Application to Application Enabled** toggle to toggle on.

-OR-

Use the following URL: `https://appliance/service/appliance/v2/A2AService/Enable`

Step 3: Asset Administrator adds assets and accounts to Safeguard for Privileged Passwords. For more information, see Adding an asset and Adding an account

Step 4: User Administrator adds certificate users to Safeguard for Privileged Passwords. For more information, see Adding a user on page 451.

Step 5: Security Policy Administrator adds application registration to Safeguard for Privileged Passwords. For more information, see Adding an application registration on page 386.

Step 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 388.

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 Safeguard for Privileged Passwords.

Prerequisites

- User Administrator adds certificate users to Safeguard for Privileged Passwords.
- Asset Administrator adds assets and accounts to Safeguard for Privileged Passwords.

To add an application registration

1. Log in to the Safeguard for Privileged Passwords desktop client as a Security Policy Administrator.
2. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Application to Application**.
3. Click **+Add**.

   The **New Registration** dialog displays.
4. On the **General** tab, 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** pane 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 388.
   d. **I want to configure this registration for**: Select the tasks to be performed by the Application to Application service:
      - **Access Request Broker**: Select this check box if you want the third-party application to create an access request on behalf of another user.
      - **Credential Retrieval**: Select this check box if you want the third-party application to retrieve credentials from the Safeguard for Privileged Passwords vault without having to go through the normal workflow process.

- **Visible to certificate user**: Select this check box to make the registration, including the API keys, visible by the certificate user that is configured for the A2A registration.

Depending on the check boxes selected, additional tabs are displayed.

5. If **Access Request Broker** is selected, 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.
6. If **Credential Retrieval** is selected, the **Credential Retrieval** tab displays a list for which the third-party can retrieve credentials from Safeguard for Privileged Passwords 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.
7. Click **Create Registration**.

Once an application registration is added to Safeguard for Privileged Passwords, the third-party application can authenticate with Safeguard for Privileged Passwords 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 388.

Deleting an application registration

Click 🗑 **Delete** on the **Application to Application** pane in the **External Integration** settings view to delete an application registration from Safeguard for Privileged Passwords.

To delete an application registration

1. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **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 Safeguard for Privileged Passwords desktop client as a Security Policy Administrator.
2. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Application to Application**.
3. Select an application registration from the list.
4. Click 🔧 from the toolbar.
5. On the **API Keys** dialog, select the API key to be replaced.
6. Click ⚙.

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 Safeguard for Privileged Passwords in the following ways:

- Credential retrieval: A third-party application can retrieve a credential from the Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords to retrieve a password or start a session.

A third-party application authenticates with Safeguard for Privileged Passwords using an API key and a client certificate, rather than the bearer token normally used to authenticate Safeguard for Privileged Passwords API requests. To make a request, you must first retrieve the API key for the application from Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords. For more information, see Adding an application registration on page 386.
- Associate the third-party application with an existing Safeguard for Privileged Passwords certificate user.

To make a credential retrieval request from the third-party application

1. Retrieve the relevant API key for the application from Safeguard for Privileged Passwords. You can retrieve the API key using the desktop client or API.

   Using the desktop client:

   - Log in to the Safeguard for Privileged Passwords client as a Security Policy Administrator.
   - Navigate to **Administration Tools** | **Settings** | **External Integration** | **Application to Application**.
   - Click to display the API keys.
   - On the **API Keys** dialog, select the API key and click .

   Using the Safeguard for Privileged Passwords API:

   - Use the following URL to retrieve the details of the registered application from the Safeguard for Privileged Passwords 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://<Appliance
     ```

```
IP>/service/core/V2/A2ARegistrations?filter=AppName%20eq%20%22<Application
Name>%22
```

- Use the ID property in the response retrieved for the application registration to retrieve the API key for the selected account from the Safeguard for Privileged Passwords API:

  ```
  https://<Appliance
  IP>/service/core/V2/A2ARegistrations/<Id>/RetrievableAccounts?filter=Accou
  ntName%20eq%20%22<account name>%22%20and%20SystemName%20eq%20%22<system
  name>%22&fields=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 Safeguard for Privileged Passwords. That is, install the trusted root certificate in Safeguard for Privileged Passwords.
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/V2/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 Safeguard for Privileged Passwords. You can retrieve the API key using the desktop client or API.

   Using the desktop client:

   - Log in to the Safeguard for Privileged Passwords client as a Security Policy Administrator.
   - Navigate to **Administration Tools** | **Settings** | **External Integration** | **Application to Application**.
   - Click to display the API keys.
   - On the **API Keys** dialog, select the API key and click .

   Using the Safeguard for Privileged Passwords API:

- Use the following URL is retrieve the details of the registered application from the Safeguard for Privileged Passwords 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://<Appliance IP>/service/core/V2/A2ARegistrations?filter=AppName%20eq%20%22<Application Name>%22
  ```

- Use the ID retrieved for the application registration to retrieve the API key from the Safeguard API:

  ```
  https://<Appliance IP>/service/core/V2/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 Safeguard for Privileged Passwords. That is, install the trusted root certificate in Safeguard for Privileged Passwords.
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 Safeguard for Privileged Passwords user that will be used to create the request. The result must uniquely identify a valid Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords user. This takes priority if it contains a value.
- ForUser: The name of a Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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.

Approval Anywhere

The Safeguard for Privileged Passwords Approval Anywhere feature integrates its access request workflow with Starling Two-Factor Authentication (2FA), allowing approvers to receive a notification through an app on their mobile device when an access request is submitted. The approver can then approve (or deny) access requests through their mobile device without needing access to the desktop or web application.

The Approval Anywhere feature is enabled when you join Safeguard for Privileged Passwords to Starling. For more information, see Starling on page 412. Once enabled, it is the responsibility of the Security Policy Administrator to define the users who are authorized to use Approval Anywhere to approve access requests. This can be done using the **Administrative Tools** | **Settings** | **External Integration** | **Approval Anywhere** pane.

> NOTE: In version 2.1 and earlier, you had to specify a Starling API key in order to use Approval Anywhere and Starling Two-Factor Authentication (2FA) as a secondary authentication provider. This is no longer necessary when you join Safeguard for Privileged Passwords to Starling. If you previously configured these features, once you join to Starling, Safeguard for Privileged Passwords automatically migrates your previous configurations to use the credential string generated by the join process.

Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Approval Anywhere**. The **Approval Anywhere** pane displays the following about the users authorized to use the Approval Anywhere feature.

Table 154: Approval Anywhere: Properties

Setting	Description
Name	Name of the Safeguard for Privileged Passwords user. NOTE: This user must also be added as an approver in an access request policy.
Mobile Phone	Valid mobile phone number in E.164 format for the authorized user.
Alternate Mobile Phone	Alternate mobile phone number in E.164 format.
Email Address	Valid email address for the authorized user.

Use these toolbar buttons to manage the users authorized to use Approval Anywhere.

Table 155: Approval Anywhere: Toolbar

Setting	Description
+ Add	Add Safeguard for Privileged Passwords users who are authorized to use this feature to approve (or deny) access requests. NOTE: Approval Anywhere approvers must have a valid mobile phone number in E.164 format and a valid email address defined. If a user does not display a valid mobile phone number or email address, edit the user record before proceeding. For more information, see Modifying a user on page 461. E.164 format: +<country code><area code><phone number> 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 Approval Anywhere.

Adding authorized user for Approval Anywhere

Once Safeguard for Privileged Passwords is joined to Starling, use the **Approval Anywhere** pane to add the Safeguard for Privileged Passwords users that can use the Approval Anywhere feature to approve access requests.

NOTE: If you upgraded from a previous version of Safeguard for Privileged Passwords where you have already configured Approval Anywhere, your existing configure will continue to work. However, you will not be able to manage your Approval Anywhere users until you join Safeguard for Privileged Passwords to Starling. Once you join to Starling, Safeguard for Privileged Passwords automatically migrates your previous configurations to use the credential string generated by the join process.

TIP: Ensure OneTouch approvals is enabled on the two-factor authentication app on your mobile device.

To add users who are authorized to use Approval Anywhere

1. Log in to the Safeguard for Privileged Passwords desktop client as a Security Policy Administrator.
2. Navigate to **Administrative Tools** | **Settings**.
3. Select **External Integration** | **Approval Anywhere**.
4. Click **+Add**.
5. In the **Users** dialog, select users from the list and click **OK**.

   NOTE: Approval Anywhere approvers must have a valid mobile phone number in

E.164 format and a valid email address defined. If a user does not display a valid mobile phone number or email address, edit the user record before proceeding. For more information, see Modifying a user on page 461.

E.164 format: +<country code><area code><phone number>

6. Add these Approval Anywhere users as approvers in the appropriate access request policy. For more information, see Creating an access request policy on page 276.

Once a user is added as an Approval Anywhere user and as an approver in an access request policy, when an access request requires approval, Safeguard for Privileged Passwords sends a notification to the approver's Starling 2FA mobile app. The approver can either approve or deny the access request directly from the Starling 2FA mobile app.

NOTE: Revoking an access request that has already been approved is not available via the mobile app. You must use the Safeguard for Privileged Passwords desktop or web client to perform that action.

Email

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

TIP: You must configure the DNS Server and set up the user's email address correctly.

To configure the SMTP Server

1. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Email**.
2. To configure the email notifications, enter these global settings for all Safeguard for Privileged Passwords emails:

SMTP Server Address	Enter the IP address or DNS name of the mail server. When unspecified, Safeguard for Privileged Passwords disables the email client. NOTE: When entering an IPv6 address, you must encapsulate it in square brackets, such as [b86f:b86f:b86f:1:b86f:b86f:b86f:b86f]. NOTE: If you are using a mail exchanger record (MX record), you must specify the domain name for the mail server.
SMTP Port	Enter the TCP port number for the email service. Default: 25 Range: 1 to 32767

Sender Email	Enter an email address to use as the "From" address for all emails originating from the appliance. Required if you specify the SMTP Server Address. Limit: 512 characters
Require Transport Layer Security	Select this option to require that Safeguard for Privileged Passwords uses TLS to provide communication security over the internet.

To validate your setup

1. Select the **Test Email Settings** link.
2. Enter a **Send To** email address of where to send the test message and click **Send**.

   Safeguard for Privileged Passwords sends an email using the configuration settings.

The grid at the bottom of this pane lists the email templates used to define the content to be included in email notifications. Use these toolbar buttons to manage email templates.

Table 156: Email template: Toolbar

Property	Description
New	Add an email template. NOTE: You can only add a previously deleted template.
Delete	Remove the selected email template.
Refresh	Update the list of email templates.
Edit	Modify the selected email template. For more information, see Modifying an email template on page 397.

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 451.

      -OR-

ii. Users set this up in their **My Account** settings. For more information, see User information and log out (desktop client) on page 86.

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 395.

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 49.

Modifying an email template

Safeguard for Privileged Passwords provides default email templates for most events, such as when a password change fails or an access request is denied. However, you can customize individual email templates, for example to provide notification when emergency access is granted .

Each template corresponds to a single event type; the event triggers an email notification that uses the template.

To modify an email template

1. Open the email template for editing. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Email** | **Email Templates**.
2. In the **Email Template** dialog:
   a. **Event**: The event is selected when adding a new template. For more information, see Enabling email notifications on page 396.
   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 Safeguard for Privileged Passwords generates the data defined by the macro within the double braces. (For more information about using macros, see note at the end of this topic.)

      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 Safeguard for Privileged Passwords generates the data defined by the macro within the double braces. (For more information about using macros, see note below.)

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.

NOTE: Each event type supports specific macros that are appropriate for that type of event. You can enter the macro into the text of the subject line or body using keywords surrounded by double braces rather than inserting the macro. However, Safeguard for Privileged Passwords ignores macros that are not supported by the event type. Unsupported macros appear blank in the email preview.

Identity and Authentication

Safeguard for Privileged Passwords 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, OpenLDAP 2.4, any SAML 2.0 federated service, or Radius.

To be managed, a directory asset must be added as both an asset and as an identity provider. When adding the identity provider, if the account name matches an account name already linked to an identity provider, the provider is automatically assigned.For more information, see Accounts on page 147.

Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Identity and Authentication**. The **Identity and Authentication** pane displays the following details about the identity and authentication providers defined.

Table 157: 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. NOTE: The Starling 2FA service provider is automatically added to Safeguard for Privileged Passwords when you join Safeguard for Privileged Passwords to One Identity Starling. You cannot manually add, edit, or delete the Starling 2FA secondary authentication provider. For more information, see Starling on page 412.
Type	Types of identity and authentication providers follow. There are valid

Property	Description
	primary and secondary authentication combinations. For more information, see Authentication provider combinations on page 399. • Active Directory • LDAP • External Federation • Radius (use as a secondary authentication provider) • Radius as Primary (use as a primary authentication provider) • FIDO2
Description	Enter any descriptive information to use for administrative purposes.

Use these toolbar buttons to manage identity and authentication provider configurations.

Table 158: 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 402.
Delete Selected	Remove the selected identity or authentication provider. The provider can be deleted if there are no associated users.
Refresh	Update the list of identity and authentication providers.
Edit	Modify the selected identity or authentication provider.
Sync Now	Run the directory addition and deletion synchronization process on demand. In addition, it runs through the discovery, if there are discovery rules and configurations set up.
Download	Download a copy of Safeguard for Privileged Passwords'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 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.

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.

NOTE: The Starling 2FA service provider is automatically added to Safeguard for Privileged Passwords when you join Safeguard for Privileged Passwords to One Identity Starling. You cannot manually add, edit, or delete the Starling 2FA secondary authentication provider. For more information, see Starling on page 412.

NOTE: 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 Safeguard for Privileged Passwords. For more information, see Requiring secondary authentication log in on page 457.

Using Local as the identity provider

Table 159: Allowable local identity provider combinations

Primary authentication	Secondary authentication
Local: The specified login name and password will be used for authentication.	None Starling Radius Active Directory LDAP FIDO2
Certificate: The specified certificate thumbprint will be used for authentication.	None Starling Radius Active Directory LDAP FIDO2
External Federation: The specified email address or name claim will be used for authentication.	None Starling 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 Starling Active Directory LDAP

Primary authentication	Secondary authentication
	FIDO2

Using Active Directory as the identity provider

Table 160: 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 Starling Radius LDAP FIDO2
External Federation: The specified email address or name claim will be used for authentication.	None Starling 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 Starling Active Directory LDAP FIDO2

Using LDAP as the identity provider

Table 161: Allowable LDAP identity provider combinations

Primary authentication	Secondary authentication
LDAP: The specified username attribute will be used for authentication.	None Starling Radius Active Directory

Primary authentication	Secondary authentication
	FIDO2
External Federation: The specified email address or name claim will be used for authentication.	None Starling 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 Starling Active Directory LDAP FIDO2

Adding identity and authentication providers

It is the responsibility of the Asset 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 a User Administrator or Appliance Administrator to create an External Federation or Radius provider to use for authentication.

To add identity and authentication providers

1. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **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.

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 or LDAP only, if applicable.

Table 162: Active Directory and LDAP: General tab properties

Property	Description
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. Safeguard for Privileged Passwords uses DNS-SRV to resolve domain names to actual domain controllers.
Network Address (for OpenLDAP)	Enter a network DNS name or the IP address of the LDAP server for Safeguard for Privileged Passwords to use to connect to the managed system over the network.
Service Account Name (for Active Directory)	Enter an account for Safeguard for Privileged Passwords to use for management tasks. If the account name matches an account name already linked to an identity provider, the provider is automatically assigned. When you add the directory, Safeguard for Privileged Passwords automatically adds the service account to the directory's **Accounts** tab and disables it for access requests. If you want the password to be available for release, click **Access Requests** and select **Enable Password Request** from the details toolbar. To enable session access, select **Enable Session Request**. Add an account that has permission to read all of the domains and accounts that you want to manage with Safeguard for Privileged Passwords. Safeguard for Privileged Passwords is forest-aware. Using the service account you specify, Safeguard for Privileged Passwords automatically locates all of the domains in the forest and creates a directory object that represents the entire forest. The directory object will have the same name as the forest-root domain regardless of which account you specify.

Property	Description
	For more information, see About service accounts on page 201.
Service Account Distinguished Name (for OpenLDAP)	Enter a fully qualified distinguished name (FQDN) for Safeguard for Privileged Passwords to use for management tasks. For example: `cn=dev-sa,ou=people,dc=example,dc=com`
Service Account Password	Enter the password Safeguard for Privileged Passwords 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.
Advanced	Open to reveal the following synchronization settings:
Available Domains for Identity and Authentication (for Active Directory)	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**. 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 473.
Port (for LDAP)	Enter port 389 used for communication with the LDAP directory.
Use SSL Encryption	Not supported.
Verify SSL Certi-ficate	Not supported.
Sync additions every	Enter or select how often you want Safeguard for Privileged Passwords to synchronize directory additions (in minutes). This updates Safeguard for Privileged Passwords with any additions, or modifications that have been made to the directory objects, including group membership and user account attributes mapped to Safeguard for Privileged Passwords. Default: 15 minutes Range: Between 1 and 2147483647
Sync deletions	Enter or select how often you want Safeguard for Privileged

Property	Description
every	Passwords to synchronize directory deletions (in minutes). This updates Safeguard for Privileged Passwords with any deletions that have been made to the directory objects, including group membership and user account attributes mapped to Safeguard for Privileged Passwords. Default: 15 minutes Range: Between 1 and 2147483647

Attributes tab

On the **Attributes** tab, synchronize the attributes in Safeguard for Privileged Passwords to the directory schema attributes. The **Attributes** tab displays the default directory attributes that are mapped to the Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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. Safeguard for Privileged Passwords' auto-complete feature immediately displays a list of attributes to choose. Safeguard for Privileged Passwords 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 163: Active Directory and LDAP: Attributes tab (defaults)

Safeguard for Privileged Passwords 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

Safeguard for Privileged Passwords attribute	Directory attribute
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 OpenLDAP 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 473.
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 OpenLDAP 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 473.
Managed Objects	The directory attribute used when automatically associating existing managed Accounts to users of a directory user group as

Safeguard for Privileged Passwords attribute	Directory attribute
	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 OpenLDAP 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 OpenLDAP 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 473.
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

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 Safeguard for Privileged Passwords user account to be associated with the federated account. 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 Safeguard for Privileged Passwords and logged in.

NOTE: Additional two-factor authentication can be assigned to the associated Safeguard for Privileged Passwords user account to force the user to authenticate again after being redirected back from the external STS.

To use external federation, you must first download the federation metadata XML for your STS and save it to a file. For example, for Microsoft's AD FS, you can download the federation metadata XML from:

https://<adfs server>/FederationMetadata/2007-06/FederationMetadata.xml.

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. **Realm**: The unique realm value (typically a DNS suffix, like contoso.com) that matches the email addresses of users that will use this STS for authentication. A case-insensitive comparison will be used on this value when performing Home Realm Discovery.
   c. **Federation Metadata File**: Click **Browse** to select the STS federation metadata xml file.
   d. **Description**: Enter any text. The text is seen only here and used for administrative purposes.
2. Click **Download Safeguard for Privileged Passwords 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. **Type**: Choose **As Primary Authentication** or **As Secondary Authentication**.
   c. **Server Address**: Enter a network DNS name or the IP address used to connect to the server over the network.
   d. **Secondary Server Address**: (Optional) Enter a network DNS name or the IP address for an additional or redundant server.

e. **Shared Secret**: Enter the server's secret key. Click to show the server's secret key.

f. **Port**: Enter the port number that the Radius server uses to listen for authentication requests. The default is port 1812.

g. **Timeout**: Specify how long to wait before a Radius authentication request times out. The default is 20 seconds.

h. **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.

i. **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.

j. **Description**: Enter any text. The text is seen only here and used for administrative purposes.

2. Click **OK**.

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**.

SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks. Safeguard for Privileged Passwords allows you to configure SNMP subscriptions for sending SNMP traps to your SNMP console when certain events occur.

Navigate to **Administrative Tools** | **Settings** | **External Integration** | **SNMP**. The **SNMP** pane displays the following about the SNMP subscribers defined.

Table 164: 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
Community	The SNMP community string being used by the SNMP subscriber
Description	The description of the SNMP subscriber
# of Events	The number of events selected to be sent to the SNMP console

Use these toolbar buttons to manage the SNMP subscriptions.

Table 165: SNMP: Toolbar

Option	Description
New	Add a new SNMP subscription. For more information, see Configuring SNMP subscriptions on page 411.
Delete Selected	Remove the selected SNMP subscription.
Refresh	Update the list of SNMP subscriptions.
Edit	Modify the selected SNMP subscription.

Option	Description
Copy	Clone the selected SNMP subscription.

Configuring SNMP subscriptions

It is the responsibility of the Appliance Administrator to configure Safeguard for Privileged Passwords to send SNMP traps to your SNMP console when certain events occur.

NOTE: To download Safeguard for Privileged Passwords 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. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **SNMP**.
2. Click **+New** 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
Events	**Browse** to select one or more SNMP event types. Use the **Clear** icon to remove an individual event from this list or right-click and select **Remove All** to clear all events from the list. NOTE: The **SNMP** pane displays the number of events that you select, not the names of the events.
Version	Choose the SNMP version: Version 1 or Version 2 Default: Version 2
Community	Enter the SNMP community string, such as public. The SNMP community string is like a user ID or 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.

Verifying SNMP configuration

Use the **Send Test Event** link located under the SNMP table on the **Settings** | **External Integration** | **SNMP** pane.

To validate your setup

1. When configuring your SNMP subscription, on the **SNMP** dialog, add the test event to your event subscription.
2. Return to the SNMP settings pane:
   a. Select the SNMP configuration from the table.
   b. Select **Send Test Event**. Safeguard for Privileged Passwords sends a test event notification to your SNMP console.

Starling

One Identity Starling Two-Factor Authentication (2FA) is a SaaS solution that provides two-factor authentication on a product allowing organizations to quickly and easily verify a user's identity. This service is provided as part of the One Identity Starling cloud platform. In addition, Starling offers a hybrid service, One Identity Hybrid, that allows you to take advantage of companion features from multiple Starling services, such as Starling Two-Factor Authentication.

Joining Safeguard for Privileged Passwords to Starling adds Safeguard to the One Identity Hybrid service allowing you to use features from the Starling 2FA services. For more information, see Join Starling on page 412.

A video of Safeguard and Starling 2FA and Approval Anywhere can be found on the Support site at One Identity Safeguard Video and Tutorials then scroll to the video, *Safeguard and Starling 2FA*.

Join Starling

In order to use Starling 2FA with Safeguard for Privileged Passwords's Approval Anywhere feature or as a secondary authentication provider, you must join Safeguard for Privileged Passwords to Starling. It is the responsibility of the Appliance Administrator to join Safeguard for Privileged Passwords to Starling.

NOTE: In version 2.1 and earlier, you had to specify a Starling API key in order to use Approval Anywhere and Starling Two-Factor Authentication (2FA) as a secondary

authentication provider. This is no longer necessary when you join Safeguard for Privileged Passwords to Starling. If you previously configured these features, once you join to Starling, Safeguard for Privileged Passwords automatically migrates your previous configurations to use the credential string generated by the join process.

For additional information and documentation regarding the Starling Cloud platform and Starling Two-Factor Authentication, see Starling Two-Factor Authentication - Technical 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:

- A valid license for Safeguard for Privileged Passwords with One Identity Hybrid subscription included.

  NOTE: You must have a valid license for Safeguard: Privileged Passwords.
- Register a Starling Organization Admin account or a Collaborator account associated with the One Identity Hybrid subscription. For more information on Starling, see the One Identity Starling User Guide.
- Download the **Starling 2FA** app on your mobile phone to use the Approval Anywhere feature.
- 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 Safeguard for Privileged Passwords for outbound web requests to integrated services, see Networking.

To sign up for a Starling One Identity Hybrid service trial account

1. Go to https://www.cloud.oneidentity.com/ and log in or register a new account for the Starling cloud platform.
   a. From the Starling home page, click **Sign in to Starling**.
   b. Enter a valid email address and click **Next**.
   c. Enter your password and click **Sign In**.
   d. On the **Create your Account** page, enter your organization and your mobile phone number.

   NOTE: If the email address you entered does not exist, you will be taken directly to the **Create your Account** page to register your organization and enter your name, password, and mobile phone number.

   When registering for the first time, you will be sent a verification email in which you must click the supplied link in order to complete the registration process.
2. Once logged in, click the **Trial** button under the **One Identity Hybrid** tile. Follow the prompts on the screen.

The service will be added to the **My Services** section and be available for use until the trial period has ended. The number of days left in your trail is indicated by a countdown at the top right of the service access button on the home page of Starling. At any point in the trial you can use the **More Information** button associated with the service to find out how to purchase the product.

Join Safeguard for Privileged Passwords with Starling

1. Navigate to **Administrative Tools** | **Settings**| **External Integration** | **Starling**. 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.
2. Click **Join to Starling**.

   NOTE: 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 Safeguard for Privileged Passwords will be joined with.

   After the join has successfully completed, you will be returned to the Safeguard for Privileged Passwords desktop client and the **Starling** settings pane will now show **Joined to Starling**. Once Starling is joined, you can configure users to require secondary authentication using Starling. For more information, see Authentication tab (add user) on page 453.

To unjoin Safeguard for Privileged Passwords from Starling

1. In **Settings**, select **External Integration** | **Starling**.
2. Click **Unjoin Starling**.

   Safeguard for Privileged Passwords will no longer be joined to Starling, which means that Approval Anywhere and two-factor authentication as a secondary authentication provider are also disabled in Safeguard for Privileged Passwords. A Starling Organization Admin account or Collaborator account associated with the Starling One Identity Hybrid subscription can rejoin Safeguard for Privileged Passwords to Starling at any time.

After the join

Once Safeguard for Privileged Passwords is joined to Starling, the following Safeguard for Privileged Passwords features are enabled and can be implemented using Starling Two-Factor Authentication:

- Secondary authentication

  Safeguard for Privileged Passwords supports two-factor authentication by configuring authentication providers, such as Starling Two-Factor Authentication, which are used to configure Safeguard for Privileged Passwords's authentication process such that it prompts for two sources of authentication when users log in to Safeguard for Privileged Passwords.

  A Starling 2FA authentication provider is automatically added to Safeguard for Privileged Passwords when you join Safeguard for Privileged Passwords to Starling. As an Authorizer or User Administrator, you must configure users to use Starling 2FA as their secondary authentication provider when logging into Safeguard for Privileged Passwords. For more information, see Configuring user for Starling Two-Factor Authentication when logging in to Safeguard on page 458.

- Approval Anywhere

  The Safeguard for Privileged Passwords Approval Anywhere feature integrates its access request workflow with Starling Two-Factor Authentication (2FA), allowing approvers to receive a notification through an app on their mobile device when an access request is submitted. The approver can then approve (or deny) access requests through their mobile device without needing access to the desktop or web application.

  Approval Anywhere is enabled when you join Safeguard for Privileged Passwords to One Identity Starling. As a Security Policy Administrator, you must define the Safeguard for Privileged Passwords users authorized to use Approval Anywhere. For more information, see Adding authorized user for Approval Anywhere on page 394.

Syslog

Safeguard for Privileged Passwords allows you to define one or more syslog servers to be used for logging Safeguard for Privileged Passwords event messages. Using this feature, Appliance Administrators can specify to send different types of messages to different syslog servers.

Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Syslog**. The **Syslog** pane displays the following about each syslog server defined.

Table 166: Syslog server: Properties

Property	Description
Network Address	The IP address or FQDN of the syslog server
Port	The UDP port number for syslog server
Facility	The type of program being used to create syslog messages
Description	The description of the syslog server configuration
# 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 167: Syslog server: Toolbar

Option	Description
New	Add a new syslog server configuration. For more information, see Configuring a syslog server on page 416.
Delete Selected	Remove the selected syslog server configuration from Safeguard for Privileged Passwords.
Refresh	Update the list of syslog server configurations.
Edit	Modify the selected syslog server configuration.
Copy	Clone the selected syslog server configuration.

Configuring a syslog server

It is the responsibility of the Appliance Administrator to configure Safeguard for Privileged Passwords to log event messages to a syslog server.

To configure a syslog server

1. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Syslog**.
2. Click **+ New** to display the **Syslog** dialog.
3. In the **Syslog** dialog, enter the following:
   a. **Network Address**: Enter the IP address or FQDN of the syslog server.
      Limit: 255 characters
   b. **UDP Port**: Enter the UDP port number for the syslog server.
      Default: 514
      Range: between 1 and 32767
   c. **Description**: Enter a description for the syslog server configuration.
      Limit: 255 characters
   d. **Events**: Click **Browse** to select the events to be included in the syslog.
      On the **Event** selection dialog, select the events to be included, then click **OK**.
   e. **Facility**: Choose the type of program to be used to log syslog messages.
      Default: User-level messages
4. Click **OK** to save your selection and add the syslog server configuration.

Verifying syslog server configuration

Use the **Send Test Event** link located below the Syslog configuration table on the **Syslog** pane to verify your syslog server configuration. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Syslog**.

To validate your setup

1. When configuring your syslog server, on the **Syslog** dialog add the test event.
2. Back on the **Syslog** pane, select the syslog server configuration from the table, then select **Send Test Event**.

   Safeguard for Privileged Passwords logs a test message to the designated syslog server.

NOTE: To log event messages to a syslog server, you must configure Safeguard for Privileged Passwords to send alerts. For more information, see Configuring alerts on page 118.

Ticketing systems

You can integrate with an external ticketing system or use ticketing that is not configured with an external ticketing system. Tickets can be viewed in the Activity Center, **Ticket #** column.

Not integrated with an external ticketing system

Security Policy Administrators can require requesters to reference a ticket number in their password 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.

Require a ticket number

1. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Ticket Systems**.
2. Click + **Add** to add a ticket system.
3. Provide the following:
   a. **Name**: Enter a name to be used in tracking tickets.
   b. **Type**: Select **Other**.
   c. **Regular Expression**: Enter the regular expression pattern to validate for an exact match. For more information, see Regular expressions on page 597.
   d. 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. For more information, see Creating an access request policy
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. For more information, see Requesting a password release and 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.

Integrated with an external ticketing system

Safeguard for Privileged Passwords allows you integrate with your company's external ticket system such as ServiceNow or Remedy. Workflow examples follow.

> IMPORTANT: The data items specific to ServiceNow and Remedy (for example, Client ID, Client Secret, and Authentication String) may be optional based on your configuration.

ServiceNow integration workflow example

ServiceNow is a cloud-based issue tracking system. Safeguard for Privileged Passwords can exchange the following ticket types with ServiceNow:

- INC (incident) tickets
- CHG (change) tickets
- RITM (request) tickets
- PRB (problem) tickets

To use ServiceNow, the root CA Certificate required for ServiceNow must be installed in Safeguard for Privileged Passwords. For more information, see Trusted Certificates on page 363. To add a trusted certificate, see Adding a trusted certificate.

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. For more information, see Creating an access request policy
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. For more information, see Requesting a password release and Requesting session access.
3. Safeguard for Privileged Passwords 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 integration workflow

The details in the ServiceNow integration workflow example apply to Remedy ticket systems except Remedy will have a different certificate and ticket types. 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.

Ticketing pane

Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Ticket Systems**. The Ticket System pane displays the following about the ticket systems defined.

Ticketing toolbar

Use these toolbar buttons to manage the ticketing systems defined to integrate with Safeguard for Privileged Passwords.

- **New**: Add a new ticket system.
- **Delete Selected**: Remove the selected ticket system from Safeguard for Privileged Passwords.
- **Refresh**: Update the list of ticket systems.
- **Edit**: Modify the selected ticket system configuration.

To configure Safeguard for Privileged Passwords to integrate with an external ticket system

1. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Ticket Systems**.
2. Click **Add** to add a new ticket system.
3. Provide the following:
   a. **Name**: Enter the name of your ticketing system.
   b. **Type**: Select the type of ticketing tracking system:
      - **ServiceNow**: A cloud-based issue tracking system.
      - **Remedy**: A request-for-service problem tracking system.
   c. **URL**: Enter the web site address to the ticketing system.
   d. **User Name**: Enter an account for Safeguard for Privileged Passwords to use to access the ticketing system.
   e. **Password**: Enter the user account's password.
   f. **Client Identifier**: Enter the ServiceNow Client ID.

g. **Client Secret**: Enter the ServiceNow secret key.

h. **Authentication String**: Enter the authentication credential for the Remedy AR (Action Request) system server.

i. **Test Connection**: Click **Test Connection** verify the connection works.

Messaging settings

Safeguard for Privileged Passwords allows you to set the following notifications.

Navigate to **Administrative Tools** | **Settings** | **Messaging**.

Table 168: Messaging settings

Setting	Description
Login Notification	Where you enable a login banner that users must acknowledge before they can access Safeguard for Privileged Passwords
Message of the Day	Where you set the **Message of the Day** that displays on the Home page

Login Notification

It is the responsibility of the Appliance Administrator to configure the login notification displayed when a user logs into Safeguard for Privileged Passwords.

To configure the login notification

1. Navigate to **Administrative Tools** | **Settings** | **Messaging** | **Login Notification**.
2. Select the **Message** check box and enter a message.
3. Click **OK**.

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, however any user with administrator permissions has the ability to set the message of the day.

To configure the message of the day

1. Navigate to **Administrative Tools** | **Settings** | **Messaging** | **Message of the Day**.

2. Choose either the **RSS** or **Subject Line** option.
3. When the **RSS** option is selected, enter a web address.
4. When the **Subject line** option is selected, enter the following information:
    - **Subject Line**: Enter a short description.
    - **Message**: Enter the text of up to 255 characters.
5. Click **OK**.

Profile settings

Use the Password settings to define the profile configuration settings, including account password rules and password check and change schedules, which can then be used in partition profile definitions.

Navigate to **Administrative Tools** | **Settings** | **Profile**.

Table 169: Profile settings

Setting	Description
Account Password Rules	Where you define the complexity rules used by Safeguard for Privileged Passwords when constructing new passwords during an automatic account password change
Change Password	Where you define the rules Safeguard for Privileged Passwords uses to reset account passwords
Check Password	Where you define the rules Safeguard for Privileged Passwords uses to verify account passwords
Password sync groups	Where you define the password sync groups and associated accounts so Safeguard for Privileged Passwords can synchronize passwords across accounts

Account Password Rules

Navigate to **Administrative Tools** | **Settings** | **Profile** | **Account Password Rules**.

Account password rules govern the construction of a new password created by Safeguard for Privileged Passwords 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 three 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: You select an account password rule set when defining a partition's profile. For more information, see Creating a profile on page 302. An account password rule applies to all accounts governed by the profile.

Navigate to **Administrative Tools** | **Settings** | **Profile** | **Account Password Rules**.

Use these toolbar buttons to manage your account password rules.

Table 170: Account Password Rules: Toolbar

Option	Description
Add Account Password Rule	Add an account password complexity rule. For more information, see Adding an account password rule on page 422.
Delete Selected	Remove the selected rule.
Refresh	Update the list of account password rules.
Edit	Modify the selected rule.
Copy	Clone the selected rule.

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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords. This causes the following issues:

- Check Password for that account will fail. When Safeguard for Privileged Passwords compares the password on the Unix host with the password in Safeguard for

Privileged Passwords, they never match because the Unix host truncated the password generated by Safeguard for Privileged Passwords.

- A user will not be able to log in to the Unix host account successfully with the password provided by Safeguard for Privileged Passwords unless they truncate the password to the allowable length imposed by the operating system.

To add an account password rule

1. Navigate to **Administrative Tools** | **Settings** | **Profile** | **Account Password Rules**.
2. Click **+ Add Account Password Rule** to open the **Account Password Rule** dialog.
3. **Browse** to select the partition.
4. Enter a Name for the account password rule (up to 50 characters).
5. Enter a **Description** for the account password rule (up to 255 characters).
6. Set the password requirements.
   - **Password Length**: Set a range for the password allowable length from three to 255 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.

- **Alpha Character**:
  - **Allow Uppercase**: Select to allow uppercase (capital) letters.
    - **Minimum of** [enter a number] **Required 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.
    - Click **Advanced** to set the following:
      - **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 **Max Allowed** value of one or more.
      - **Excluded 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.
    - **Minimum of** [enter a number] **Required 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.
    - Click **Advanced** to set the following:
      - **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 **Max Allowed** value of one or more.
      - **Excluded 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 **Max Allowed**.

    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.
- **Numeric Character**:
  - **Allow Numeric (0-9)**: Select to allow numeric characters in the password.
    - **Minimum of** [enter a number] **Required Numbers**: Enter a number to identify the amount of numbers required in a password. To allow but not require numbers, set this value at zero.

- Click **Advanced** to set the following:
  - **Limit Consecutively Repeated Numeric Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated numbers. You must enter a **Max Allowed** value of one or more.
  - **Excluded Characters**: Enter any numbers (0 though 9) you want to exclude from the password.

- **Alphanumeric Characters**
  - **Limit Consecutively Repeated Alphanumeric Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated alphanumeric characters. You must enter a **Max Allowed** value of one or more.
- **Symbols**:
  - **Allow Symbols (e.g. @ # $ % &)**: Select this check box to allow characters that are printable ASCII characters. These often include: ~ ` ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
  - **Minimum of** [enter number] **Required Symbols**: Enter a number to identify the least number of symbols required. To allow but not require symbols, set this value at zero.
  - Click **Advanced** to set the following:
    - **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 **Max Allowed** value of one or more.
    - **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.

7. Click **Test Rule** to check the rules set.
8. When the rules are complete, click **OK**.

Change Password

Change password settings are the rules Safeguard for Privileged Passwords uses to reset account passwords.

Navigate to **Administrative Tools** | **Settings** | **Profile** | **Change Password**.

The **Change Password** pane displays the following about the listed change password setting rules.

Table 171: 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 172: Change Password: Toolbar

Option	Description
Add Change Password Setting	Add a change password rule. For more information, see Adding change password settings on page 426.
Delete Selected	Remove the selected rule.
Refresh	Update the list of change password rules.
Edit	Modify the selected rule.
Copy	Clone the selected rule.

Adding change password settings

It is the responsibility of the Asset Administrator or the partition's delegated administrator to configure the rules Safeguard for Privileged Passwords 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 432.

To add a password reset schedule

1. Navigate to **Administrative Tools** | **Settings** | **Profile** | **Change Password**.
2. Click **Add Change Password Setting** to open the **Change Password Settings** dialog.
3. **Browse** to select a partition.
4. Enter a **Name** of up to 50 characters for the rule.
5. Enter a **Description** of up to 255 characters for the rule.

6. Optionally, select any of the following:
    - **Manage Password**: Select this option to allow Safeguard for Privileged Passwords to rotate the password it uses to communicate with an asset configured to use SSH Key Authentication. For more information, see SSH Key on page 203.
    - **Manage SSH Key**: Select this option to allow Safeguard for Privileged Passwords to rotate the SSH key it uses to communicate with an asset configured to use SSH Key Authentication. For more information, see SSH Key on page 203.
    - **Change Passwords Manually**. For more information, see How do I manage accounts on unsupported platforms on page 564.
7. After **Change Password**, click the link or click the **Schedule** button.
8. 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.
        - **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 **-** delete 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 AM**
- **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 that 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 20:00:00 PM** and **Repeat 2**.

- **Time Zone**: Select the time zone.

9. Optionally, complete any of these settings:
   - **Change the Password Even if a 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 (supported platforms)**: 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 Safeguard for Privileged Passwords, at which time Safeguard for Privileged Passwords 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.
   - **Update Service on Password Change (Windows Only)**: For dependent accounts assigned to an asset that run system services, select this option to ensure that the password change is also applied to each service the account runs. The asset's profile setting is used. This overrides the profile assigned to the account. If you have a local account, the profile assigned to the account overrides the profile assigned to the asset when updating dependent services on the same appliance.
   - **Restart Service on Password Change (Windows Only)**: For dependent accounts assigned to an asset that run system services, select this option to ensure that there is an automatic restart after the password is changed. The asset's profile setting is used. This overrides the profile assigned to the account. If you have a local account, the profile assigned to the account overrides the profile assigned to the asset when updating dependent services on the same appliance.

- **Update IIS App Pools on Password Change (Windows Only)**: For dependent accounts that run IIS App pools, select this option to ensure that the password change is also applied to each IIS App pool the account runs.
- **Update COM+ on Password Change (Windows Only)**: For dependent accounts that run COM+ applications, select this option to ensure that the password change is also applied to each COM+ application the account runs.
- **Update Task on Password Change (Windows Only)**: For dependent accounts that run scheduled system tasks, select this option to ensure that the password change is also applied to each task the account runs.

  NOTE: When managing passwords for Windows service accounts, do not select this option. Create a separate Profile with Change Password settings that do not have this option selected for managing Windows service accounts.
- **Manage Password**: Select this option to allow Safeguard for Privileged Passwords to rotate the password it uses to communicate with an asset configured to use SSH Key Authentication. For more information, see SSH Key on page 203.
- **Manage SSH Key**: Select this option to allow Safeguard for Privileged Passwords to rotate the SSH key it uses to communicate with an asset configured to use SSH Key Authentication. For more information, see SSH Key on page 203.
- **Details**: Click to see the Knowledge Base article to learn which systems and platform combinations are supported.

Check Password

Check password settings are the rules Safeguard for Privileged Passwords uses to verify account passwords.

Navigate to **Administrative Tools** | **Settings** | **Profile** | **Check Password**.

The **Check Password** pane displays the following about the listed check password setting rules.

Table 173: 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 174: Check Password: Toolbar

Option	Description
Add Check Password Setting	Add a check password rule. For more information, see Adding check password settings on page 430.
Delete Selected	Remove the selected rule.
Refresh	Update the list of check password rules.
Edit	Modify the selected rule.
Copy	Clone the selected rule.

Adding check password settings

It is the responsibility of the Asset Administrator or the partition's delegated administrator to define the rules Safeguard for Privileged Passwords uses to verify account passwords.

To add a password validation schedule

1. Navigate to **Administrative Tools** | **Settings** | **Profile** | **Check Password**.
2. Click **Add Check Password Setting** to open the **Check Password Settings** dialog.
3. **Browse** to select a partition.
4. Enter a **Name** of up to 50 characters for the rule.
5. Enter a **Description** of up to 255 characters for the rule.
6. Click the **Schedule** button 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.
        - **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 **-** delete 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 AM**
  - **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 that 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 20:00:00 PM** and **Repeat 2**.

- **Time Zone**: Select the time zone.

8. Optionally, complete either of these settings:

   - **Change Password on Mismatch**: Select this option to automatically change a password when Safeguard for Privileged Passwords detects the password in the appliance database differs from the password on the asset.
   - **Notify Delegated Owners on Mismatch**: Select this option to trigger a notification when Safeguard for Privileged Passwords detects a password mismatch.

     NOTE: To send event notifications to a user, you must configure Safeguard

for Privileged Passwords to send alerts. For more information, see Configuring alerts on page 118. Set up an email template for the Password Check Mismatch event type.

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 partition 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 profile on page 302.

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 master system is set at priority 0 and the subordinates are set at priority 1, the password change on the master must be successful before the passwords on the subordinates are changed. If the master password change fails, the subordinates are unaffected, the cluster continues to function, password change is rescheduled, and the error is logged.

Navigate to **Administrative Tools** | **Settings** | **Profile** | **Password Sync Groups**. The **Password Sync Groups** pane displays the following for each sync group.

Table 175: Sync Groups: Properties

Property	Description
Enable	If **Enable** is selected, the sync runs with the Partition 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.
Partition	The partition that uses the rule.
Profile	The profile that uses the rule.
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 partition profile. See Creating a profile.

Table 176: Sync Groups: Toolbar

Option	Description
Add	Add a password sync group. For more information, see Adding a password sync group on page 433.
Delete Selected	Permanently remove the selected password sync group.
Refresh	Update the list of password sync groups.
Edit	Modify the selected password sync group rule. For more information, see Modifying a password sync group on page 434.
Change Sync Group Password	Change the password for the selected sync group. All accounts in the password sync group synchronize with the new password.

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 profile.

To create a password sync group

1. Navigate to **Administrative Tools** | **Settings** | **Profile** | **Password Sync Groups**.
2. Click **+ Add** to open the **Password Sync Group** dialog.
3. Click **Browse** to select a Profile. The **Profile** name displays.

   NOTE: 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 . For more information, see Password sync group account priority on page 432.
4. Enter a **Name** of up to 100 characters.
5. Enter a **Description** of up to 255 characters.
6. Click **+Add** and select one or more **Accounts** to be synchronized.

   The **Accounts** list displays with the following information about the account: **Name**, **Parent**, **Service Account**, **Needs a Password** (if yes or if no), and **Description**. Click any columns to sort the accounts.
7. Click **OK**. 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, enter the new priority, and click **OK**. For more information, see Password sync group account priority on page 432.
   - **System Name**: Name of the system (asset) assigned that is associated with the account.
   - **Account Name**: Name of the account.
   - **Last Sync Time**: The date and time of the last sync.
8. Click **OK**.

Modifying a password sync group

You can make modifications to the account priority within a password sync group, the accounts assigned to a password sync group, or sync the selected account password.

To modify the account priority of a password sync group or perform other modifications

1. Navigate to **Administrative Tools** | **Settings** | **Profile** | **Password Sync Groups**.
2. In the **Password Sync Group** dialog, select the password sync group, then click **Edit**.
3. Modify the **Name** or **Description**, if desired.
4. Click any column in the account list to sort the accounts.
5. To modify an account priority, select the account then click **Edit**.
6. Enter the **Priority**, then click **OK**. For more information, see Password sync group account priority on page 432.
7. Perform any of the following account modifications:
   - Click **+ Add** to add an account to the password sync group.
   - Click **Remove Selected** to remove the selected account from the password sync group. This does not delete the account from Safeguard for Privileged Passwords.
   - Click **Refresh** to update the account list.
   - Click **Sync Now** to sync the selected account password to match the sync group password. The **Status** follow:
     - displays when the account password is in sync with the password sync group.
     - displays if the password is not in sync.

Safeguard Access settings

Safeguard for Privileged Passwords allows you to configure these settings related to accessing Safeguard for Privileged Passwords. Navigate to **Administrative Tools** | **Settings** | **Safeguard Access**.

Table 177: Safeguard for Privileged Passwords Access settings

Setting	Description
Login Control	Where you configure the user login control settings
Password Rule	Where you configure user password complexity rules
Time Zone	Where you can set the time zone

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. Navigate to **Administrative Tools** | **Settings** | **Safeguard Access** | **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 Safeguard for Privileged Passwords. 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**, Safeguard for Privileged Passwords 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.

	Default: Five consecutive failures TIP: 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 Safeguard for Privileged Passwords 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
Disable After	Set the number of days to wait before automatically disabling an inactive user account. If a user has not logged onto Safeguard for Privileged Passwords this number of days, Safeguard for Privileged Passwords 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
Inform User of Disabled Account	Select this option to inform users when Safeguard for Privileged Passwords has disabled their account when they attempt to log in. When cleared, Safeguard for Privileged Passwords tells the user that his or her access has been denied. NOTE: For security reasons, One Identity recommends leaving this option cleared, unless you are troubleshooting login and authentication problems. A disabled user cannot sign into Safeguard for Privileged Passwords until an administrator has re-enabled his or her account. For more information, see Enabling or disabling a user on page 461. Default: Not set
Inform User of Locked Account	Select this option to inform users when Safeguard for Privileged Passwords has locked their account when they attempt to log in. When cleared, Safeguard for Privileged Passwords tells the user that his or her 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 Safeguard for Privileged Passwords until the **Lockout Duration** period has been met or an administrator has unlocked the account. For more information, see Unlocking a user's account on page 466. Default: Not set
Minimum Password Age	Set the number of days a user must wait before changing his or her 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 Safeguard for Privileged Passwords begins to remind the user that their password is about to expire. Range: 0 to 30 days Default: 14 days
Password History	Enter the number of old passwords stored by Safeguard for Privileged Passwords 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

Password Rule

Navigate to **Administrative Tools** | **Settings** | **Safeguard Access**| **Password Rule** .

Password rules define the complexity requirements for user authentication to Safeguard for Privileged Passwords. 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 Safeguard for Privileged Passwords 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 465.

Related Topics

Account Password Rules

Modifying user password requirements

It is the responsibility of the Authorizer Administrator to configure the user password rules.

To configure user password rules

1. Navigate to **Administrative Tools** | **Settings** | **Safeguard Access** | **Password Rules**.
2. Set the **Password Length** from 3 to 255 characters.

   Default: 8 to 64 characters

   NOTE: The maximum length must be equal to or greater than the sum of minimum characters described in the next step.
3. Set the character **Requirements**:
   - **Password Length**: Set a range for the password allowable length from three to 255 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.
- **Alpha Character**:
  - **Allow Uppercase**: Select to allow uppercase (capital) letters.
    - **Minimum of** [enter a number] **Required 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.
    - Click **Advanced** to set the following:
      - **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 **Max Allowed** value of one or more.
      - **Excluded 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.
    - **Minimum of** [enter a number] **Required 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.
    - Click **Advanced** to set the following:
      - **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 **Max Allowed** value of one or more.
      - **Excluded 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 **Max Allowed**.

  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.

- **Numeric Character**:
  - **Allow Numeric (0-9)**: Select to allow numeric characters in the password.
    - **Minimum of** [enter a number] **Required Numbers**: Enter a number to identify the amount of numbers required in a password. To allow but not require numbers, set this value at zero.
    - Click **Advanced** to set the following:
      - **Limit Consecutively Repeated Numeric Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated numbers. You must enter a **Max Allowed** value of one or more.
      - **Excluded Characters**: Enter any numbers (0 though 9) you want to exclude from the password.
- **Alphanumeric Characters**
  - **Limit Consecutively Repeated Alphanumeric Characters**: If you allowed repeated characters earlier, select the check box to limit the number of consecutively repeated alphanumeric characters. You must enter a **Max Allowed** value of one or more.
- **Symbols**:
  - **Allow Symbols (e.g. @ # $ % &)**: Select this check box to allow characters that are printable ASCII characters. These often include: ~ ` ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /
  - **Minimum of** [enter number] **Required Symbols**: Enter a number to identify the least number of symbols required. To allow but not require symbols, set this value at zero.
  - Click **Advanced** to set the following:
    - **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 **Max Allowed** value of one or more.
    - **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 OK.

Time Zone

Safeguard for Privileged Passwords 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 **Administrative Tools** | **Settings** | **Safeguard Access** | **Time Zone**.
2. Select the time zone in the **Default User Time Zone** drop-down menu.

21

Users

A user is a person who can log in to Safeguard for Privileged Passwords. 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.

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, User Groups , Partitions, Entitlements, Linked Accounts, History
- Asset Administrator: General, Partitions
- Security Policy Administrator: General, User Groups , Entitlements, Linked Accounts, History

The Authorizer Administrator typically controls the **Enabled/Disabled** state. For more information, see Enabling or disabling a user on page 461.

The **Users** view displays the following information about a selected user:

- General 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.
- Partitions tab (user): Displays the partitions over which the selected user is a delegated partition administrator.
- Entitlements tab (user): Displays the entitlements in which the selected user is a member; that is, an entitlement "user".
- Linked Accounts tab (user): Displays the directory accounts linked to the selected user.
- History (user): Displays the details of each operation that has affected the selected user.

Use these toolbar buttons to manage users:

- **Add User**: Add users to Safeguard for Privileged Passwords. For more information, see Adding a user on page 451.
- **Delete Selected**: Remove the selected user. For more information, see Deleting a user on page 462.
- **Refresh**: Update the list of users.
- **Import Users**: Add users to Safeguard for Privileged Passwords. For more information, see Importing objects on page 462.
- **User Security**: Menu options include: **Set Password** and **Unlock** accounts. For more information about these options, refer to Setting a local user's password and Unlocking a user's account.
- **Permissions**: Display the **Permissions** dialog showing what administrative permissions apply to the selected user.
- **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 111.

General tab (user)

The **General** tab lists information about the selected user.

Large tiles at the top of the tab display the number of **User Groups**, **Partitions**, **Entitlements**, and **Linked Accounts** associated with the selected user, based on the user's permissions. Clicking a tile heading opens the corresponding tab.

The tiles visible depend on your administrator permissions:

- All tiles are visible to the Auditor.
- **Partitions** tile is visible to Asset Administrator.
- **User Groups**, **Entitlements**, and **Linked Accounts** tiles are visible to Security Policy Administrator.

Table 178: Users General tab: Authentication properties

Property	Description
Identity	
Identity Provider	The source from which the user’s personal information comes from and is synchronized with.

Property	Description
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 Address	The user's email address.
Authentication	
Authentication Provider	How the user authenticates with Safeguard for Privileged Passwords: • **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.
Location	
Time Zone	The user's geographic location.
Permissions	
Permissions	Lists the user's administrator permissions or "Standard User" if user does not have administrative permissions.
Description	
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.

Related Topics

Modifying a user

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).

Table 179: Users: Users Groups tab properties

Property	Description
Name	The user group name
Type	The type of group: **User Group** or **Directory Group**
Distinguished Name	The distinguished name of the group
Description	Information about the selected user group

Use the following buttons on the details toolbar to manage the user groups associated with the selected user.

Table 180: Users: User Groups toolbar

Option	Description
Add User Group	Add the user to one or more user groups to the user. For more information, see Adding a user to user groups on page 459.
Remove Selected	Remove the selected user group from the selected user.
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 111.

Partitions tab (user)

The **Partitions** tab displays the partitions over which the selected user is a delegated partition administrator. The **Partitions** tab is available to a user with Auditor or Asset

Administrator permissions.

Table 181: Users: Partitions tab properties

Property	Description
Name	The partition name
Description	Information about the selected partition.

Use the following buttons on the details toolbar to manage the partitions associated with the selected user.

Table 182: Users: Partitions toolbar

Option	Description
Assign Partition(s)	Delegate the selected user as an administrator to one or more partitions. For more information, see Assigning a user to partitions on page 459.
Remove Selected	Remove the selected partition from the selected user.
Refresh	Retrieve and display an updated list of partitions associated with the selected user.
Search	To locate a specific partition in this list, enter the character string to be used to search for a match. For more information, see Search box on page 111.

Related Topics

Assigning a user to partitions

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.

Table 183: Users: Entitlements tab properties

Property	Description
Name	The name of the entitlements in which the selected user is assigned as a user.
Access Request 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 287.

Use the following buttons on the details toolbar to manage the entitlements associated with the selected user.

Table 184: Users: Entitlements tab toolbar

Option	Description
Add Entitlement	Add the selected user as a user of one or more entitlements. For more information, see Adding a user to entitlements on page 459.
Remove Selected	Remove the user from the selected entitlement.
Refresh	Update the list of entitlements.
Details	View additional details about the selected entitlement in a pop-up window.
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 111.

Linked Accounts tab (user)

The **Linked Accounts** tab displays the directory accounts linked to the selected user that can be used in session request policies to access the assets or accounts defined within the

scope of the policy.

Accounts can be:

- Manually: Click **+Add Linked Account** from the details toolbar.
- Automatically: See Adding a directory user group and the check box labeled **Automatically link Managed Directory Accounts**.

Table 185: Users: Linked Accounts tab properties

Property	Description
Name	The account name.
Domain Name	The name of the domain where the linked account resides.
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.
Needs a Password	Displays ⚠ if a password is not set for the account. For more information, see Checking, changing, or setting an account password on page 165.
Description	Information about the selected account.

Use the following buttons on the details toolbar to manage the linked accounts associated with the selected user.

Table 186: Users: Linked Accounts tab toolbar

Option	Description
+Add Linked Account	Link the user to one or more accounts. For more information, see Linking a directory account to a user on page 460.
−Remove Selected	Remove the selected linked account from the selected user.
Refresh	Update the list of linked accounts.
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 111.

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).

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.
- **Search**: For more information, see Search box on page 111.
- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Table 187: 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 • 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.

Select an event to display this additional information for some types of events (for example, create and update events).

Table 188: Additional History tab properties

Property	Description
Property	The property that was updated
Old Value	The value of the property before it was updated
New Value	The new value of the property

Managing users

Use the controls and tabbed pages on the Users page to perform the following tasks to manage Safeguard for Privileged Passwords users:

- Adding a user
- Requiring secondary authentication log in
- Adding a user to user groups
- Assigning a user to partitions
- Adding a user to entitlements
- Linking a directory account to a user
- Modifying a user
- Deleting a user
- Importing objects
- Setting a local user's password
- Unlocking a user's account
- Enabling or disabling a user

Adding a user

It is the responsibility of either the Authorizer Administrator or the User Administrator to add Safeguard for Privileged Passwords users.

To add a user

1. Navigate to **Administrative Tools** | **Users**.
2. In **Users**, click **+ Add 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.
    - Location tab (add user): Where you set the user's time zone.
    - Permissions tab (add user): Where you set the user's administrator permissions.

Related Topics

Adding users or user groups to an entitlement

Adding users to a user group

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, Safeguard for Privileged Passwords 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 398.

Table 189: User: Identity tab properties

Property	Description
Identity Provider	The source of the user's identity. Safeguard for Privileged Passwords comes with a built-in identity provider called **Local** that will allow you to manually enter user information that is stored directly in Safeguard for Privileged Passwords. Or you can select an Active Directory or LDAP server that you have previously configured and then browse for a user. Safeguard for Privileged Passwords will periodically synchronize with the directory to keep the information up to date. Indicate how the user's identity is managed by Safeguard for Privileged Passwords: • Local • Active Directory • LDAP
Browse (Active Directory or	If the identity provider is Active Directory or LDAP, click the **Browse** button to choose a username. The remaining fields are auto-populated.

Property	Description
LDAP)	
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
Mobile Phone (**Local** provider)	Enter the user's mobile telephone number. Limit: 30 characters NOTE: A valid mobile phone number in E.164 format is required for approvers using the Approval Anywhere feature and for two-factor authentication using Starling. However, you can use the **Use alternate mobile phone number** option on the **Authentication** tab to specify a valid mobile phone number, instead of adding it here. E.164 format: +*<country code><area code><phone number>*
Email Address (**Local** provider)	Enter the user's email address. Limit: 255 characters NOTE: Required for approvers using the Approval Anywhere feature and for two-factor authentication using Starling.
Description (**Local** provider)	Enter information about this user. Limit: 255 characters.

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 398.

Table 190: User: Authentication tab properties

Property	Description
Authentication Provider	Indicates how this user is to authenticate to Safeguard for Privileged Passwords. The options are: • **Certificate**: With a certificate

Property	Description
	NOTE: Safeguard for Privileged Passwords 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 49. • **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 Safeguard for Privileged Passwords, such as Active Directory or LDAP, and the identity provider of the user is also that directory). • *<External Federation service provider name>*: With the credentials required by the External Federation or Radius server (only available if one or more of those authentication providers have been configured in Safeguard for Privileged Passwords).
Login name (**Local** or **Radius as Primary**)	If using **Local** or **Radius as Primary** for authentication, enter the user's login name. If using directory authentication, the login name is auto-populated.
Set Password (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 Password Rule on page 438.
Certificate Thumbprint (SHA-1) (**Certificate** user)	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.
Email Address or Name Claim (external federation)	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. Safeguard for Privileged Passwords 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 Safeguard for

Property	Description
	Privileged Passwords according to what claim is returned by your STS, with precedence given to the email address claim.
Require Certificate Authentication (**Active Directory** provider)	Select this check box to require that the user logs into Safeguard for Privileged Passwords using their domain issued user certificate or SmartCard. NOTE: 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.
Require Secondary Authentication	Select this check box to require that this user logs in to Safeguard for Privileged Passwords with two-factor authentication. For more information, see Requiring secondary authentication log in on page 457. 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 398.
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 Safeguard for Privileged Passwords 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 408. A best practice is to have the users log in to validate the correct user is set up.
Use alternate mobile phone number (if Starling Two-Factor Authentication)	When Starling Two-Factor Authentication is selected, this option is available to enter an alternate **Mobile phone number**. The Number on file is the mobile phone number specified on the user's **Identity** tab. NOTE: The Approval Anywhere and one-touch approval features require a valid mobile phone number for the user. If the user does not have their mobile number published in Active Directory, use this option to specify a valid mobile phone number for the user.

Location tab (add user)

On the Location tab, specify the user's time zone.

Table 191: User: Location tab properties

Property	Description
Time Zone	Select the user's time zone. NOTE: Because Microsoft Active Directory does not have a Time Zone attribute, when you add a directory group, Safeguard for Privileged Passwords sets the default time zone 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.

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 directory user groups

Users have permissions based on the directory user groups to which they are assigned. If a user is removed from a directory 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 473.

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, Ticketing, and Approval Anywhere.
- Operations: Allow the user to reboot and monitor the appliance.
- Auditor: Allow the user read-only access.
- 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.

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 **Settings** | **External Integration** | **Identity and Authentication**. For more information, see Adding identity and authentication providers on page 402. Or, you may use Starling 2FA. For more information, see Starling on page 412.
2. Configure the Safeguard for Privileged Passwords user to **Require Secondary Authentication**. For more information, see Authentication tab (add user) on page 453.
   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 Safeguard for Privileged Passwords with two-factor authentication.
3. Log in with secondary authentication.

   When you log in to Safeguard for Privileged Passwords as a user which requires secondary authentication, you log in as usual, using the password that is set for the Safeguard for Privileged Passwords user account. Safeguard for Privileged Passwords 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, One Identity Starling Two-Factor Authentication, 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 Safeguard for Privileged Passwords with secondary authentication.

For more information, see To manage your FIDO2 keys on page 86.

Configuring user for Starling Two-Factor Authentication when logging in to Safeguard

It is the responsibility of the Authorizer Administrator or the User Administrator to configure a user account to use two-factor authentication when logging in to Safeguard for Privileged Passwords.

TIP: If you want to use one-touch approvals, download and install the **Starling 2FA** app onto your mobile device.

To configure users to use Starling Two-Factor Authentication when logging in to Safeguard for Privileged Passwords

1. Log in to Safeguard for Privileged Passwords as an Authorizer Administrator or User Administrator.
2. Navigate to **Administrative Tools** | **Users**.
3. Add or edit users, ensuring the following settings are configured:
   a. Authentication tab:
      - **Require Secondary Authentication:** Select this check box.
      - **Authentication Provider**: Select the **Starling 2FA** service provider.

        NOTE: If the **Starling 2FA** service provider is not listed, you must first join Safeguard for Privileged Passwords to Starling. For more information, see Starling on page 412.
      - **Use alternate mobile phone number**: Optionally, select this check box and enter an alternate mobile number to be used for two-factor authentication notifications.

        NOTE: If you want to use one-touch approvals, this feature requires a valid mobile phone number for the user. If the user does not have their mobile number published in Active Directory, use this option to specify a valid mobile phone number for the user.

   b. Contact Information tab:
      - **Mobile Phone**: Enter a valid mobile phone number in E.164 format.
      - **Email Address**: Enter a valid email address.

Now whenever any of these users attempt to log in to Safeguard for Privileged Passwords, after entering their password, a message appears on the login screen informing them that an additional authentication step is required.

NOTE: If the Safeguard for Privileged Passwords user is required to use Starling Two-Factor Authentication and has the **Starling 2FA** mobile app installed, Safeguard for Privileged Passwords sends a push notification to their mobile device where they can complete the login by pressing a button in the app. If the user does not have the **Starling 2FA** app, they have the option to receive a one-time password via SMS or a phone call.

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 **Administrative Tools** | **Users**.
2. In **Users**, select a user from the object list and open the **User Groups** tab.
3. Click **+ Add User Groups** 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 selection dialog and add the user group. For more information about creating user groups, see Adding a user group.

Assigning a user to partitions

It is the responsibility of the Asset Administrator to select one or more users to manage the assets and accounts in a partition. Assigning a user to a partition makes that user the delegated owner of that partition, giving that person authorization to manage the assets and accounts in that partition. A delegated partition owner has a subset of the permissions that an Asset Administrator has. For more information, see Administrator permissions on page 507.

To assign a user to partitions

1. Navigate to **Administrative Tools** | **Users**.
2. In **Users**, select a user from the object list and open the **Partitions** tab.
3. Click **+ Assign Partition(s)** from the details toolbar.
4. Select one or more partitions from the list in the **Partitions** selection dialog and click **OK**.

If you do not see the partition you are looking for and are an Asset Administrator, you can click **+ Create New** in the **Partitions** dialog. For more information about creating partitions, see Adding a partition.

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 **Administrative Tools** | **Users**.
2. In **Users**, select a user 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 list in the **Entitlements** selection 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.

Linking a directory account to a user

It is the responsibility of the Security Policy Administrator to link directory accounts 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 a directory account to a user

1. Navigate to **Administrative Tools** | **Users**.
2. In **Users**, select a user from the object list and open the **Linked Accounts** tab.
3. Click **+ Add Linked Account** from the details toolbar.

   The **Directory Account** dialog displays, listing the directory accounts available in Safeguard for Privileged Passwords. This dialog includes the following details about each directory account listed:

   - **Name**: Displays the name of the directory account.
   - **Domain Name**: Displays the name of the domain where this account resides.
   - **Service Account**: A check mark indicates the account is a service account.
   - **Password Request**: A check mark indicates password release requests are allowed.
   - **Session Request**: A check mark indicates the account is enabled for session requests.
   - **Needs a Password**: Indicates whether the account needs a password.
   - **Description**: Displays descriptive text about the directory account.
4. Select one or more accounts from the list in the **Directory Account** selection dialog and click **OK**.

Related Topic

Adding an account

Modifying a user

The Authorizer Administrator can modify the General information for a user. The User Administrator can modify the General information for a Help Desk User. Other administrators can view information for users.

You cannot modify a directory user's contact information that is managed in the directory, such as Active Directory. If you need to add a valid mobile phone number, use the alternate mobile phone number option on the **Authentication** tab instead.

> TIP: As a best practice, if you change a user's administrative permissions, ensure the user closes all connections to the appliance (or reboot the appliance) to prevent users from gaining access to information.

To modify a user

1. Navigate to **Administrative Tools** | **Users**.
2. In **Users**, select a user. Perform the following, as needed.

- On the **General** tab, click the **Edit** icon next to **Identity**, **Authentication**, **Location**, and **Permissions** or double-click the user's name to open the **User** dialog and update the information on the tabs.
- On the **User Group** tab, the Security Policy Administrator can modify a user's group membership. You can multi-select user groups to add or remove more than one user on a user's group membership.
- On the **Partitions** tab, the Asset Administrator can delegate partition ownership to a user.
- On the **Entitlements** tab, the Security Policy Administrator can add the selected user to an entitlement.
- On the **Linked Accounts** tab, the Security Policy Administrator can add (or remove) linked accounts associated with the user to link the user to an entitlement.
- Right-click the user and select **Permissions** to change permissions.
- The Authorizer Administrator and the User Administrator can view or **Export** the details of each operation that has affected the selected use on the **History** tab. For more information, see History (user) on page 450.

Enabling or disabling a user

Typically, it is the responsibility of the Authorizer Administrator to enable or disable administrator users and the User Administrator to enable or disable non-administrator users. You can modify a disabled user's information. If a directory user is disabled in the directory asset, the user cannot be enabled in Safeguard.

Disabling a user prevents from logging in to Safeguard for Privileged Passwords; however, if you disable a directory user, that does not prevent that user from logging in to the directory.

When re-enabling a disabled account, the Authorizer Administrator must reset the user's password. Simply enabling the account does not permit the user to log in with the previous password.

You configure the number of days you want Safeguard for Privileged Passwords to wait before automatically disabling an inactive user account in the **Disable After** Login Control Setting. For more information, see Login Control on page 436.

To enable or disable a user

1. Navigate to **Administrative Tools** | **Users**.
2. In **Users**, select a user from the object list.
3. In the upper-right corner of the window, click **Enabled** (toggle on) or **Disabled** (toggle off) to toggle to the setting.

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, Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords will add it back in. As a best practice, disable the directory user instead of deleting the account. For more information, see Enabling or disabling a user on page 461.

To delete a user

1. Navigate to **Administrative Tools** | **Users**.
2. In **Users**, select a user from the object list.
3. Click **Delete Selected**.
4. Confirm your request.

Importing objects

Safeguard for Privileged Passwords 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. For more information, see Creating an import file on page 164.

Once an import is completed, you can navigate to the **Tasks** pane in the Toolbox for details about the import process and invalid data messages. For more information, see Viewing task status on page 145.

To import objects

1. In **Administrative Tools**, click **Assets**, **Accounts**, or **Users** based on what data you are importing.
2. Click **Import** from the toolbar.
3. In the **Import** dialog, **Browse** to select an existing .csv file containing a list of objects to import.
4. When importing assets, the **Discover SSH Host Keys** option is selected by default indicating that Safeguard will retrieve the required SSH host key for the assets specified in the .csv file.
5. Click **OK**.

   Safeguard for Privileged Passwords imports the objects into its database.

   NOTE: Safeguard for Privileged Passwords does not add an object if any column contains invalid data in the .csv file, with the following exceptions:

   - Assets **PlatformDisplayName** property:
     1. If Safeguard for Privileged Passwords does not find an exact match, it looks for a partial match. If it finds a partial match, it supplies the ***<platform>*** **Other** platform, such as **Other Linux**.
     2. If it does not find a partial match, it supplies the **Other** platform type.
   - Users **TimeZoneId** property:
     1. If Safeguard for Privileged Passwords does not find a valid TimeZoneId property (that is, does not find an exact match or no time zone was provided), it uses the local workstation's current time zone.

        NOTE: Do not enter numbers or abbreviations for the TimeZoneId.
   - Users **Password** property:
     1. Safeguard for Privileged Passwords adds a user without validating the password you provide.

Details for importing directory assets, service accounts, users, and user groups

You can use the steps like those above to import your existing directory infrastructure (such as Microsoft Active Directory). Managed account users cannot be members of the Protected Users AD Security Group.

Additional information specific to directory import follows.

1. Import the directory (and service account) via **Administrative Tools** | **Assets** | **Import Asset** and browse to select the .csv file. Safeguard for Privileged Passwords imports the directory as an asset.

   The directory's service account is automatically added to the list of accounts you can viewed via the **Assets** | **Accounts** tab.

   - By default, the service account password is automatically managed according to the check and change settings in the profile that governs the partition. For

more information, see Creating a profile on page 302. If you do not want Safeguard for Privileged Passwords to manage the service account password, assign the account to a profile that is set to never change passwords. For more information, see Assigning assets or accounts to a profile on page 305.

- The service account is added to the asset's Accounts tab and is disabled for password request and session request. For more information, see Accounts tab (asset) on page 186.
- To change either setting, navigate to **Administrative Tools** | **Accounts** and double-click the account. Then select the following check boxes, as desired: **Enable Password Request** and **Enable Session Request**. For more information, see General tab (account) on page 148.

2. Import users and user groups.

   a. Import directory users via **Administrative Tools** | **Users** | **Import Users** and browse to select the .csv file.

   b. Assign to user groups via **Administrative Tools** | **Users Groups** | **Users** (select one or multiple users).

   c. Automatic synchronization: Once you import directory users and directory groups, Safeguard for Privileged Passwords automatically synchronizes the objects in its database with the directory schema attributes. User and group membership changes in the directory are reflected in Safeguard for Privileged Passwords. Directory users authenticate to Safeguard for Privileged Passwords with their directory credentials.

Active Directory and LDAP synchronization

Active Directory and LDAP data is automatically synchronized by asset or identity and authentication providers schema as shown in the following lists.

Asset schema list

- Users
  - Username
  - Password (modifiable in LDAP and not modifiable in Active Directory)
  - Description
- Groups
  - Name
  - Member
- Computer
  - Name
  - Network Address
  - Operating System
  - Operating System Version
  - Description

Identity and Authentication Providers schema list

- Users
    - Username
    - First Name
    - Last Name
    - Work Phone
    - Mobile Phone
    - Email
    - Description
    - External Federation Authentication
    - Radius Authentication
    - Managed Objects
- Groups
    - Name
    - Members
    - Description

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 **Administrative Tools** | **Users**.
2. Select a local user from the object list and perform one of the following:
    - Right-click, and select **Set Password** from the context menu.
    - Click **User Security** and select **Set Password**.
    - On the **General** tab next to **Authentication**, click **Edit** and click **Set Password**.
3. In the **Set Password** dialog, enter the new password and click **OK**. You must comply with the password requirements specified in the dialog. For more information, see Password Rule on page 438.

Unlocking a 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, Safeguard for Privileged Passwords locks your account. For more information, see Login Control on page 436.

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 user's account

There are two ways to unlock a user account:

- In **Users**, select a "locked" user, right-click, and select **Unlock** from the context menu.
- Click **User Security** and select **Unlock**.

22

User Groups

Safeguard for Privileged Passwords allows you to add both local user groups (a set of local users) and directory groups (a set of directory accounts) to User Groups. The Security Policy Administrator can add a group of users to an entitlement to authorize them 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, and the Auditor. However, it is only available to the Authorizer Administrator and User Administrator if a directory has been added to Safeguard for Privileged Passwords.

The User Groups view displays the following information about the selected user or directory group.

- General 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 to which the users associated with the selected user group are users.
- History (user): Displays the details of each operation that has affected the selected group.

Use these toolbar buttons to manage users.

Add User Groups: Add user groups to Safeguard for Privileged Passwords. For more information, see Adding a user group on page 472.

Add Directory Group: Add a directory user group to Safeguard for Privileged Passwords. For more information, see Adding a directory user group on page 473.

Delete Selected: Remove the selected user group. For more information, see Deleting a user group on page 478.

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 111.

Related Topics

Modifying a user group

Adding users or user groups to an entitlement

General tab (user groups)

The **General** tab lists information about the selected user group.

Large tiles at the top of the tab display the number of **Users** in the selected group and, when applicable, the number of **Entitlements** to which the selected group is an entitlement member or user. Clicking a tile heading opens the corresponding tab.

> NOTE: The **Entitlements** tile is only visible to the Auditor and Security Policy Administrator.

Navigate to **Administrative Tools** | **User Groups** | **General**.

Table 192: User Groups General tab: General properties

Property	Description
Name	The group name.
Distinguished Name (directory user group)	The distinguished name of the group.
Primary Authentication Provider (directory user group)	The name of the authentication provider (for example, the name of an external provider such as a Microsoft Active Directory domain name).
Permissions (directory user group)	Lists the user's administrator permissions or "Standard User" if user does not have administrative permissions.

Related Topics

Modifying a user group

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.

Navigate to **Administrative Tools** | **User Groups** | **Users**.

Table 193: User Groups: Users tab properties

Property	Description
User Name	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.
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.

Use these buttons on the details toolbar to manage the users in your user groups.

Table 194: 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 476.
Remove Selected	Remove the selected user from the user group.
Refresh	Update the list of users in the user groups.
Details	View additional details about the selected user.
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 111.

Related Topics

Adding users to a user group

Modifying a user group

Entitlements tab (user groups)

The **Entitlements** tab displays the entitlements to which the users associated with the selected user group are users.

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.

Navigate to **Administrative Tools** | **User Groups** | **Entitlements**.

Table 195: 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.
Access Request 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 196: User Groups: Entitlements tab toolbar

Option	Description
+Add Entitlement	Add the selected user group to one or more entitlements. For more information, see Adding a user group to an entitlement on page 477.
−Remove Selected	Remove the user group from the selected entitlement.
Refresh	Update the list of entitlements.
Details	View additional details about the selected entitlement.
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 111.

Related Topics

Adding a user group to an entitlement

Modifying a user group

History tab (user groups)

The **History** tab allows you to view or export the details of each operation that has affected the selected group.

The top of the **History** tab contains the following information:

- **Items**: Total number of entries in the history log.
- **Refresh**: Update the list displayed.
- **Export**: Export the data to a .csv file.
- **Search**: For more information, see Search box on page 111.
- **Time Frame**: By default, the history details are displayed for the last 24 hours. Click one of the time intervals at the top of the grid to display history details for a different time frame. If the display does not refresh after selecting a different time interval, click **Refresh**.

Navigate to **Administrative Tools** | **User Groups** | **History**.

Table 197: 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.
Related Object	The name of the related object

Property	Description
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

Select an event to display this additional information for some types of events (for example, create and update events).

Table 198: Additional History tab properties

Property	Description
Property	The property that was updated
Old Value	The value of the property before it was updated
New Value	The new value of the property

Managing user groups

Use the controls and tabbed pages on the User Groups page to perform the following tasks to manage Safeguard for Privileged Passwords user groups:

- Adding a user group
- Adding a directory user group
- Adding users to a user group
- Adding a user group to an entitlement
- Modifying a user group
- Deleting a user group

Adding a user group

It is the responsibility of the Security Policy Administrator to add groups of local users to Safeguard for Privileged Passwords.

NOTE: It is the responsibility of the Authorizer Administrator or the User Administrator to add directory groups. For more information, see Adding a directory user group on page 473.

To add a user group

1. Navigate to **Administrative Tools** | **User Groups**.
2. Click **+ Add User Groups** from the toolbar.
3. In the **User Groups** 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

Related Topics

Adding users to a user group

Adding a directory user group

An Asset Administrator (or delegate) must:

1. Add a directory asset.
2. Add the domain as an identity provider via **Settings** | **External Integration** | **Identity and Authentication**. For more information, see Identity and Authentication on page 398.

Next, the Authorizer Administrator or the User Administrator can add directory user groups.

The Security Policy Administrator can add local user groups. For more information, see Adding a user group on page 472.

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. For example, if you set the directory user group authentication properties to require secondary authentication and use the Starling 2FA provider, each user's email address and mobile phone number attributes must have values to be included during the import.

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 user group, Safeguard for Privileged Passwords sets the default time zone 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 **Administrative Tools** | **User Groups**.
2. Click **+Add Directory Group** from the toolbar.
3. In the **Directory Group** tab:
   a. Select a directory.
   b. In the **Contains** field, enter a full or partial directory group name and click **Search**.

      To search for a directory group, you must enter text into the search box. The text search is not case-sensitive and does not allow wild cards. Safeguard for Privileged Passwords 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."
   c. **Browse** to select a container within the directory as the **Filter Search Location**.
   d. 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.
   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. For details on linked accounts, see Linked Accounts tab (user).

      Based on the setting of the directory asset'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 **Administrative Tools** | **Settings** | **External Integration** | **Identity and Authentication**. For more information, see Available Domains for Identity and Authentication (for Active Directory) on page 404.

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 402.

   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. For example, their mobile phone attribute must contain a valid phone number in E.164 format when using Starling 2FA as the secondary authentication provider.

   i. Select the **Require Secondary Authentication** check box. For more information, see Requiring secondary authentication log in on page 457.

   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 398.

5. On the **Permissions** tab, select any administration permissions to be assigned to each member of the user group. 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. A user's permissions include all permissions for every directory user group to which they are assigned. For more information, see the Permissions tab (add user) under Managing Users.

When rerunning a directory user group import or during the periodic directory synchronization, a Safeguard user may be identified as no longer a member of a directory user group that was imported. In this case, the administrator permissions assigned to the group are removed from the user, regardless of whether they were added to the user during the group import process or if they were manually added to the user. If the user is a member of another directory user group, any overlapping administrator permissions will remain assigned to the user.

> IMPORTANT: Any user imported through a directory group will not have Directory permissions. You will need to manually assign the user to a partition. For more information, see Partitions tab (user) on page 446.

6. Click **Add Group**. 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 the Security Policy Administrator to associate both local or directory users to user groups. User groups belong to the identity group.

You can not add or remove users to or from a directory user group. This has to be done in Active Directory on the Directory Group object represented.

Directory group membership is still maintained in the directory, such as Active Directory.

To add users to a user group

1. Navigate to **Administrative Tools** | **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** selection dialog and click **OK**.

   > IMPORTANT: You cannot add a group to a user group's membership; group membership cannot be nested.

If you do not see the user you are looking for and you have Authorizer Administrator or User Administrator permissions, you can click **+Create New** to create users. For more information, see Adding a user.

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 **Administrative Tools** | **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** selection dialog and click **OK**.

If you do not see the entitlement you are looking for and you have Security Policy Administrator permissions, you can click **+Create New** and add the entitlement. For more information about creating entitlements, see Adding an entitlement.

Modifying a user group

Only the Security Policy Administrator can modify user groups.

To modify a user group

1. Navigate to **Administrative Tools** | **User Groups**.
2. In **User Groups**, select a user group.
3. Select the view of the user group's information you want to modify (**General**, **Users**, or **Entitlements**).

   For example:

   - To change a local user group's name or description, double-click the **General** information box on the **General** tab or click the **Edit** icon.

     NOTE: You can double-click a user group name to open the **General** settings edit window.

   - To add (or remove) users to the selected local user group, click the **Users** tab. You can multi-select members to add or remove more than one from a user group.

- To add (or remove) the selected user group to an entitlement, click the **Entitlements** tab.

4. To view or export the details of each operation that has affected the selected user group, switch to the **History** tab. For more information, see History tab (user groups) on page 471.

Deleting a user group

It is the responsibility of the Security Policy Administrator to delete groups of local users from Safeguard for Privileged Passwords. It is the responsibility of the Authorizer Administrator or the User Administrator to delete directory groups.

When you delete a user group, Safeguard for Privileged Passwords does not delete the users associated with it.

To delete a user group

1. Navigate to **Administrative Tools** | **User Groups**.
2. In **User Groups**, select a user group from the object list.
3. Click 🗑 **Delete Selected**.
4. Confirm your request.

23

Disaster recovery and clusters

Safeguard for Privileged Passwords Appliances 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 Safeguard for Privileged Passwords 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. You can perform password change and check operations and make password release and session access requests. Users can log in to replicas to request access, generate reports, or audit the data. Also, passwords 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 502.
- 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 502.

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 502.

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 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 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 485.
- 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 492.
- 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 318.
- Restart an appliance. For more information, see Restarting the appliance on page 319.

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 491.
- 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 495.

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 483.
- 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 492.

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 497.

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 desktop client. For more information, see Performing a factory reset on page 498.
- The Recovery Kiosk. For more information, see Factory reset from the Recovery Kiosk on page 553.
- The virtual appliance Support Kiosk. For more information, see Support Kiosk on page 58.

Enrolling replicas into a cluster

Prior to the Appliance Administrator enrolling cluster members into a Safeguard for Privileged Passwords 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 486.
- 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 releases and session access.
- To enroll an appliance into a cluster, the appliance must communicate over port 655 UDP/TCP and port 443 TCP, and must have IPv4 or IPv6 network addresses (not mixed).For more information, see Safeguard ports on page 580.
- 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 Safeguard for Privileged Passwords.

  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. In **Administrative Tools**, navigate to **Settings** | **Cluster** | **Cluster Management**.
4. Click **+ Add Replica** to join a Safeguard for Privileged Passwords 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. Safeguard for Privileged Passwords connects to the replica and displays the login screen for the replica appliance.
   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.

   Safeguard for Privileged Passwords 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.

   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 make access requests.
7. 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

Safeguard for Privileged Passwords allows the Appliance Administrator to unjoin replica appliances from a cluster. Prior to unjoining a replica from a Safeguard for Privileged

Passwords 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 491. 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 497.
- 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 492.

To unjoin a replica from a cluster

1. Log in to an appliance in the cluster, as an Appliance Administrator.
2. In **Administrative Tools**, navigate to **Settings** | **Cluster** | **Cluster Management**.
3. In the cluster view (left pane), select the replica node to be unjoined from the cluster.
4. In the details view (right pane), click **Unjoin**.
5. In the Unjoin confirmation dialog, enter the word **Unjoin** and click **OK** to proceed.

   Safeguard for Privileged Passwords 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 in the cluster view (left pane).

NOTE: If you log in to the replica appliance using the desktop client while Safeguard for Privileged Passwords is processing an unjoin operation, you will see the Maintenance mode screen. At the end of the Maintenance mode, you will see a **Restart Desktop Client** button, indicating that the unjoin operation completed successfully.

Maintaining and diagnosing cluster members

When a node is selected in the Cluster view (left pane) of the **Cluster** settings page, the appliance details and cluster health view (right 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 483.
- **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 491.
- **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 492.

  CAUTION: Activating an appliance that is in Read-Only mode will take it out of the Read-only state and enable password check and change for managed accounts. Ensure that no other Safeguard for Privileged Passwords 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 information. For more information, see Appliance Information on page 315.
  - Run diagnostic tests against the appliance. For more information, see Network Diagnostics on page 323.
  - Perform a factory reset. For more information, see Factory Reset from the desktop client on page 320.
  - View or edit networking settings. For more information, see Networking on page 326.
  - Generate a support bundle. For more information, see Support bundle on page 330.
  - View or edit time settings. For more information, see Time on page 330.
- **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 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 in Offline Workflow Mode

- In Offline Workflow Mode, the appliance is enabled to request, approve, and release passwords 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, the Access Request Password Reset By-passed Event is generated, stating: `An access request subsequent check out is available as password reset was by-passed.`
- Password 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 from the primary or another replica on the cluster with consensus; password check and changes works as usual. The result is that passwords may get out of sync on the appliance running Offline Workflow Mode. This is expected behavior and the password 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 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 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 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 work flow 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-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 in Safeguard are returned to the Home page. Password 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 view pane on page 367.

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 502.
- 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 and IsSessionsRequestAvailable properties. The following API endpoint can be used to make this determination:

  https://<hostname or IP>/service/notification/v2/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 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 374.
- 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 374.

To manually enable Offline Workflow Mode

1. Navigate to **Administrative Tools** | **Settings** | **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 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. Navigate to **Administrative Tools** | **Settings** | **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 Desktop Client**. 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

Safeguard for Privileged Passwords 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 497.

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. In **Administrative Tools**, select **Settings** | **Cluster** | **Cluster Management**.
3. In the cluster view (left pane), select the replica node that is to become the new primary.
4. In the details view (right pane), 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 Safeguard for Privileged Passwords 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 497.

> **CAUTION: Activating an appliance that is in Read-Only mode will take it out of the Read-only state and enable password check and change for managed accounts. Ensure that no other Safeguard for Privileged Passwords 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. In **Administrative Tools**, navigate to **Settings** | **Cluster** | **Cluster Management**.

   The cluster view (left pane) displays one primary appliance with a yellow warning icon indicating the appliance is in a Read-only mode.
3. In the cluster view (left pane), select the read-only node to be activated.
4. In the details view (right pane), 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 (left pane) 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. In **Settings**, select **Cluster** | **Cluster Management**.
2. From the cluster view (left pane), select the appliance to be diagnosed.
3. In the details pane (right pane), click **Diagnose**.

The Appliance Information view displays.

4. Select **Diagnostics** and choose the type of test to be performed.
   - Ping: To verify your network connectivity and response time.
   - NS Lookup: To obtain your domain name or IP address.
   - Trace Route: To obtain your router information; trace route determines the paths packets take from one IP address to another.
   - Telnet: To access remote computers over TCP/IP networks like the internet.
   - Show Routes: To retrieve routing table information.
5. Enter the requested information in the test dialog that displays.

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 Safeguard for Privileged Passwords 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.
- 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

> IMPORTANT: The following procedure applies to Safeguard for Privileged Passwords Appliances running version 2.1.x and later. If you need to patch appliances running an earlier version, you will need to unjoin replica appliances, install the patch on each appliance, and then enroll the replica appliances to rebuild your cluster. For more information, see Patching cluster members in the *Safeguard for Privileged Passwords 2.0 Administration Guide*.

1. Log in to the primary appliance, as an Appliance Administrator.
2. In **Administrative Tools**, select **Settings** | **Appliance** | **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. Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords 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 (**Settings** | **Cluster** | **Cluster Management**) shows that an update operation is in progress and the cluster members that are locked, awaiting to install the update file.

   In addition, the **Updates** view (**Settings** | **Appliance** | **Updates**) shows the cluster members involved in the update operation and the progress as cluster members are successfully updated.

About cluster patching

The following information provides insight into how Safeguard for Privileged Passwords 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 check out

The policy may be configured such that a password reset is required before the password 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 check out when a password has not been reset.

- The policy can be set to allow multiple accesses.
- The policy can be set to not require a password change at check in.
- Emergency requests can be allowed so the user does not have to wait for the password 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. Restore the backup on the appliance that will be the primary.
3. 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. In **Administrative Tools**, select **Settings** | **Backup and Restore**.
3. Click **+Run Now** to create a copy of the data currently on the primary appliance.

   For more information, see Run Now on page 350.

   Or you can click **Backup Settings**, in the upper-right corner of the Backups page, to configure an automatic backup schedule.

   For more information, see Backup settings on page 350.

To restore a physical appliance from a backup

An Appliance Administrator can restore backups as far back as Safeguard for Privileged Passwords version 2.2.0.6958. Only the data is restored; the running version is not changed.

If the administrator attempts to restore a version earlier than 2.2.0.6958, a message like the following displays: `Restore failed because the backup version '[version]' is older than the minimum supported version '2.2.0.6958' for restore.`

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. In **Administrative Tools**, select **Settings** | **Backup and Restore**.
3. Select the backup to be used and click **Restore**.
4. When the **Restore** dialog displays, enter the word **Restore** and click **OK**.

   For more information, see Restore on page 353.

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. In **Administrative Tools**, navigate to **Settings** | **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 492.
3. One at a time, enroll the replica appliances to rebuild your cluster.
   a. In **Administrative Tools**, select **Settings** | **Cluster**.
   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 482.

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 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 374.

To reset a cluster

1. Navigate to **Administrative Tools** | **Settings** and select **Cluster**.
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 Safeguard for Privileged Passwords 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 Desktop Client**.
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 492.

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 Safeguard for Privileged Passwords 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 Appliance Information settings page in the desktop client, from the Recovery Kiosk, from the virtual appliance Support Kiosk, or using the API.

A Safeguard for Privileged Passwords 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 66.

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. 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 68.

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 you are using version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, you appliance will reset down to 6.0 LTS and you will have to patch up to your current version. For more information, see Long Term Support (LTS) and Feature Releases on page 46.

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 68.

To perform a factory reset from the desktop client

1. Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Factory Reset**.
2. Click **Factory Reset**.
3. In the Factory Reset confirmation dialog, enter the words **Factory Reset** and click **OK**.

   The appliance will go into Maintenance mode to revert the appliance. Once completed, you will be prompted to restart the desktop client. 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 68. In addition, when you log in to the appliance, you will be prompted to add your Safeguard for Privileged Passwords licenses.

To perform a factory reset from the Recovery Kiosk

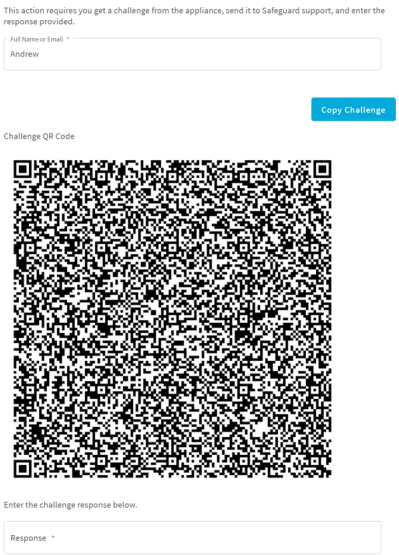
1. To perform a hardware factory reset, go to the Recovery Kiosk. For more information, see Recovery Kiosk (Serial Kiosk) on page 549.
2. Select **Factory Reset**.
3. Press the right arrow.
4. At **id**, enter your email or name and press the **Tab** key (or down arrow).
5. At **Get Challenge**, press the **Enter** key. Safeguard for Privileged Passwords

produces a challenge.

6. Copy and paste the challenge and send it to One Identity Support.
   - A challenge response is only good for 48 hours.
   - Do not navigate away from the page or refresh during a challenge response operation. Doing so will invalidate the challenge response.
7. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select **Factory Reset**.

To perform a factory reset from the Support Kiosk

1. To perform a hardware factory reset, gon the web management console, click **Support Kiosk**. For more information, see Support Kiosk on page 58.
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. Do not refresh your screen.
      - Screenshot the QR code and send it to Support. Support will send back a challenge response that is good for 48 hours. Do not refresh your screen.
      - 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, Safeguard for Privileged Passwords locks the cluster while a cluster operation is running, such as enroll, unjoin, failover, patch, reset, and routine maintenance. The Cluster view shows that the cluster is locked and that any changes to the cluster configuration are not allowed until the operation completes. The banner that appears at the top of the screen explains the operation in progress and a red lock icon (🔒) next to an appliance indicates that the appliance is locking the cluster.

To unlock a locked cluster

1. Click the 🔒 lock icon in the upper right corner of the warning banner.
2. 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 terminate 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. Most often, it will eventually time out and unlock on its own.

Troubleshooting tips

If there is a problem with a Safeguard for Privileged Passwords 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 492.
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 549.
   - Generate and collect support bundles for each appliance in the cluster and contact support. For more information, see Support bundle on page 330.

Appliance states

The following table lists the appliance states and what actions are available when the appliance is in a particular state.

Table 199: 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 42.
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) 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.	Wait for operation to complete before logging in to appliance.
Offline Appliance is not available for access.	Wait for appliance to come back online before logging in.
Offline Workflow The appliance is not communicating	Enable Offline Workflow Mode. Once online operations are resumed, the appliance is

Appliance state and description	Actions available
with the cluster but has been either automatically or manually placed in Offline Workflow Mode to run access request workflow.	returned to Maintenance mode. For more information, see About Offline Workflow Mode on page 486.
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 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 state and description	Actions available
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 549.
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.
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	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 can be

Appliance state and description	Actions available
consensus.	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 reset is required before the password 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 check out when a password has not been reset. • The policy can be set to allow multiple accesses. • The policy can be set to not require a password change at check in. • Emergency requests can be allowed so the user does not have to wait for the password 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.
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

Appliance state and description	Actions available
	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 549.

24

Administrator permissions

To secure control of your IT department's assets (that is, managed systems), Safeguard for Privileged Passwords uses a role-based access control hierarchy. Safeguard for Privileged Passwords'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 Safeguard for Privileged Passwords 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
- 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 55.
- 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 management services.

Table 200: Appliance Administrator: Permissions

Navigation	Permissions
Activity Center	View and export appliance activity events.
Administrative Tools | **Toolbox**	Access to the Tasks pane.
Administrative Tools | **Settings**:	
• **Access Request** | **Enable or Disable Services**	Enable or disable the access request and password management services.
• **Appliance**	Monitor the status of the appliance. Shut down or restart the appliance. Run diagnostics on the appliance. Enable or disable Lights Out Management (BMC). Configure networking settings. Perform a factory reset to recover from major problems or clear the data and configuration settings on the appliance. Generate a support bundle to assist technical support. Manage appliance time. Install update files (patches).
• **Appliance** | **Enable or Disable Services**	Enable or disable the Application to Application (A2A) service. Enable or disable SPP audit data to be sent to SPS for auditing the Safeguard privileged management software suite.
• **Backup and Retention**	Configure backup and retention settings, define archive servers, and manage backups.
• **Certificates**	Manage the certificates used by Safeguard.
• **Cluster**	Create and manage a clustered environment. Monitor the status of the clustered environment. Diagnose cluster members.
• **External Integration**	Configure Approval Anywhere service for access request approvals.

Navigation	Permissions
	Configures email to send event notifications to external systems. Configure identity providers and authentication providers. Configures the sending of SNMP traps to the SNMP console. Join Safeguard for Privileged Passwords to Starling. Configure Safeguard for Privileged Passwords to send event notifications to a syslog server. Configure the integration with an external ticketing system or generic tickets not tied to an external ticketing system.
• **Messaging**	Configure login notifications. Set message of the day.
• **Safeguard Access**	Configure the user login control settings, inactivity timeout, and password rules. View time zone.
• **Sessions**	If a Sessions appliance is joined, view, remove, or modify the configuration.

Asset Administrator permissions

An Asset Administrator manages all partitions, assets, and accounts:

- Creates (or imports) assets and accounts.
- Creates partitions and partition profiles.
- Delegates partition ownership to users.

  NOTE: 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.

NOTE: Asset Administrators can only view the user object history for their own account.

Table 201: Asset Administrator: Permissions

Navigation	Permissions
Dashboard | **Account**	Full control for accounts related to all Safeguard for

Navigation	Permissions
Automation	Privileged Passwords assets. NOTE: Delegated partition owners have control for accounts related to the assets managed through delegated partition profile.
Activity Center	View and export asset activity events.
Administrative Tools | **Toolbox**	Access to the Accounts, Assets, Partitions and Users view. Access to the Tasks pane.
Administrative Tools | **Accounts**	Add, modify, delete, and import accounts. Check, change, and set account passwords. Access password archive. Enable or disable the access request services for an account.
Administrative Tools | **Assets**	Add, modify, delete, and import assets. Configure and manage Asset Discovery jobs. Download SSH Key.
Administrative Tools | **Discovery**	Create and run discovery jobs to find assets, accounts, and services in your network environment.
Administrative Tools | **Partitions**	Add, modify, and delete partitions and partition profiles. Set partition as default. Add assets to the scope of a partition profile.
Administrative Tools | **Settings**:	
• **Asset Management** | **Custom Platforms**	Add a custom platform that includes uploading the custom platform script.
• **Asset Management** | **Tags**	Create and manage dynamic tags for assets and asset accounts.
• **Messaging** | **Message of the Day**	Login notification: View only. Set message of the day.
• **Profile** | **Account Password Rules**	Add, modify, and delete account password complexity rules.
• **Profile** | **Change Password**	Add, modify, and delete change password settings.

Navigation	Permissions
• **Profile** | **Check Password**	Add, modify, and delete check password settings.
• **Profile** | **Password Sync Groups**	Add, modify, and delete password sync groups.
Administrative Tools | **Users**	Delegate partition ownership to users.

Auditor permissions

The Auditor administrator has read-only access to all features, giving him the ability to review all access request activity:

- Monitors appliance information.
- Reviews everything.
- Exports object history.
- Runs entitlement reports.

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.`

Table 202: Auditor administrator: Permissions

Navigation	Permissions
Dashboard	View only.
Activity Center	View and export activity events. Audit access request workflow.
Reports	View and export entitlement reports.
Administrative Tools | **Toolbox**	Access to all Administrative Tools views and the Tasks pane.
Administrative Tools | **Accounts**	View only.
Administrative Tools | **Account Groups**	View only.
Administrative Tools | **Assets**	View Asset Discovery jobs.
Administrative Tools | **Asset Groups**	View only.
Administrative Tools | **Entitlements**	View only.

Navigation	Permissions
Administrative Tools | **Partitions**	View only.
Administrative Tools | **Settings**:	
• **Access Request**	View only.
• **Appliance**	View Appliance Information. Run diagnostics on appliance. View licensing information. View Lights Out Management (BMC) settings. View Networking settings. View Time settings. View update history.
• **Asset Management**	View only.
• **Backup and Retention**	View only.
• **Certificates**	View only.
• **Cluster**	View only.
• **External Integration**	View only.
• **Messaging**	Login notification: View only. Set message of the day.
• **Profile**	View only.
• **Safeguard Access**	View only.
Administrative Tools | **Users**	View only.
Administrative Tools | **User Groups**	View only.

Authorizer Administrator permissions

The Authorizer Administrator is the permissions administrator and performs the following:

- Creates (or imports) Safeguard for Privileged Passwords users.
- Grants administrator permissions to users.
- Sets passwords, unlocks, and enables or disables both local and directory user

accounts.

- Creates and maintains the Password Rule.

NOTE: 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.

Table 203: Authorizer Administrator: Permissions

Navigation	Permissions
Activity Center	View and export user activity events, including authentication events.
Administrative Tools | **Toolbox**	Access to the Users and User Groups view. Access to Tasks pane.
Administrative Tools | **Settings**	
• **External Integration** | **Identity and Authentic-ation**	Add, update, and delete directories used for identity and authentication. External Federation and Radius providers can be configured for authentication use.
• **Messaging** | **Message of the Day**	Login notification: View only. Set message of the day.
• **Safeguard Access** | **Login Control**	View only.
• **Safeguard Access** | **Password Rules**	Configure user password rules.
• **Safeguard Access** | **Time Zone**	View time zone.
Administrative Tools | **Users**	Add, modify, delete, and import users. Set administrator permissions. Set passwords and unlock users. Delete users. Enable or disable users.
Administration Tools | **User Groups**	Add or delete directory groups, if a directory has been added to Safeguard for Privileged Passwords.

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.

Table 204: Help Desk Administrator: Permissions

Navigation	Permissions
Activity Center	View and export user activity events.
Administrative Tools | **Toolbox**	Access to the Users view and the Tasks pane.
Administrative Tools | **Settings**:	
• **Messaging** | **Message of the Day**	Login notification: View only. Set message of the day.
• **Safeguard Access** | **Login Control**	View only.
• **Safeguard Access** | **Password Rules**	View only.
• **Safeguard Access** | **Time Zone**	View only.
Administrative Tools | **Users**	Unlock and set passwords for non-administrator users. A Help Desk Administrator can unlock another Help Desk user but cannot set that user's password.

Operations Administrator permissions

The Operations Administrator view access to the information available to the Appliance Administrator. The Operations Administrator also can take backups, reboot the appliance, and monitors the status of 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.

Table 205: Operations Administrator: Permissions

Navigation	Permissions
Activity Center	View and export appliance activity events.
Administrative Tools | **Toolbox**	Access to the Tasks pane.
Administrative Tools | **Settings**:	
• **Access Request** | **Enable or Disable Services**	View only.
• **Appliance**	Monitor the status of the appliance. Shutdown or restart the appliance. Generate a support bundle to assist technical support. View licensing information. View Networking settings. Edit operating system license. View Time settings.
• **Backup and Retention**	In a future release, only take a backup. It may appear the Operations Admin can edit data, but the change cannot be saved. • Archive server • Audit log management • Backup and restore (only take a backup) • Backup retention
• **Certificates**	View only.
• **Cluster**	View only. Monitor the status of the clustered environment.
• **External Integration**	View only. For Identity and Authentication, the grid displays but the details are not available.
• **Messaging**	Login notification: View only. Set message of the day.
• **Safeguard Access**	View only.

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 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.`

Table 206: Security Policy Administrator: Permissions

Navigation	Permissions
Dashboard | **Access Requests**	Full control to manage access requests.
Activity Center	View and export security-related activity events, including access request events. Audit access request workflow.
Reports	View and export entitlement reports.
Administrative Tools | **Toolbox**	Access to the Account Groups, Asset Groups, Entitlements, Users, and User Groups view. Access to the Tasks pane.
Administrative Tools | **Account Groups**	Add, modify, or delete account groups. Add accounts to account groups. Assign policies to account groups.
Administrative Tools | **Asset Groups**	Add, modify, or delete asset groups. Add assets to asset groups. Assign policies to asset groups.
Administrative Tools |	Add, modify, or delete entitlements.

Navigation	Permissions
Entitlements	Add users or user groups to entitlements. Define and maintain access request policies. Assign policies to entitlements.
Administrative Tools | **Settings**:	
• **Access Request** | **Reasons**	Add, modify, or delete reason codes.
• **Cluster** | **Session Appliances**	If Safeguard for Privileged Passwords (SPP) is joined to Safeguard for Privileged Sessions (SPS), view the appliance information for the join.
• **External Integration** | **Application to Application**	Add, modify, or delete application registrations.
• **External Integration** | **Approval Anywhere**	Configure Approval Anywhere service for access request approvals.
• **External Integration** | **Starling**	If Safeguard for Privileged Passwords is joined to Starling, view the Starling join information.
• **External Integration** | **Ticket Systems**	If Safeguard for Privileged Passwords is configured to use tickets (generic tickets or with an external ticketing system), view the ticket information.
• **Messaging** | **Message of the Day**	Login notification: View only. Set message of the day.
Administrative Tools | **Users**	Add users to user groups. Add users to entitlements. Link directory accounts to a user. View and export the history of users.
Administrative Tools | **User Groups**	Add, modify, or delete local user groups. Add local or directory users to user groups. Assign entitlements to user groups.

User Administrator permissions

The User Administrator:

- Creates (or imports) Safeguard for Privileged Passwords users.
- 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.

NOTE: User Administrators cannot modify administrator passwords, including their own.

IMPORTANT: 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.

Table 207: User Administrator: Permissions

Navigation	Permissions
Activity Center	View and export user activity events.
Administrative Tools | **Toolbox**	Access to the Users and User Groups view. Access to Tasks pane.
Administrative Tools | **Settings**:	
• **External Integration** | **Identity and Authentic-ation**	View only.
• **Messaging** | **Message of the Day**	Login notification: View only. Set message of the day.
• **Safeguard Access** | **Login Control**	View only.
• **Safeguard Access** | **Password Rules**	View only.
• **Safeguard Access** | **Time Zone**	View only.
Administrative Tools | **Users**	Add, modify, delete or import local and directory users. Set passwords and unlock accounts for non-administrator users. A Help Desk Administrator can unlock another Help Desk user but cannot set that user's passwrod. Enable or disable non-administrative users. Set Help Desk Administrator permissions.
Administrative Tools | **User Groups**	Add or delete directory groups, if a directory has been added to Safeguard for Privileged Passwords.

25

Preparing systems for management

Before you add systems to Safeguard for Privileged Passwords (Adding an asset on page 193), you must ensure they are properly configured.

Generally, to prepare an asset for Safeguard for Privileged Passwords:

1. Create a functional account (called a "service" account in Safeguard for Privileged Passwords) on the asset and assign it a password.

   NOTE: To add an asset to Safeguard for Privileged Passwords, it must have a service account. For more information, see About service accounts on page 201.

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 Safeguard for Privileged Passwords. For more information, see Trusted Certificates on page 363.

The following topics can help you prepare your hosts for management by Safeguard for Privileged Passwords:

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 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 Windows SSH systems

Safeguard for Privileged Passwords supports a variety of platforms. For more information, see Supported platforms on page 37.

Preparing ACF - Mainframe systems

This applies to both ACF2 - Mainframe and ACF2 - Mainframe LDAP platforms.

To prepare IBM ACF-mainframe systems for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the z/OS system using password authentication.

About certificate support for the telnet protocol

Safeguard for Privileged Passwords automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, Safeguard for Privileged Passwords does not support client certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, Safeguard for Privileged Passwords cannot support that configuration.

Preparing Amazon Web Services platforms

Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords

1. In Safeguard for Privileged Passwords:
    a. Add Amazon's certificate and AWS certificate's root certificate authority (CA) to the Trusted Certificates store in Safeguard for Privileged Passwords.
    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 Safeguard for Privileged Passwords.

Preparing Cisco devices

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.

To prepare a Cicso device for Safeguard for Privileged Passwords

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. Configure the **Privilege Level Password** (that is, the system enable password). This password is required when adding the asset to Safeguard for Privileged Passwords.

   NOTE: Safeguard for Privileged Passwords manages accounts found in the startup configuration file, not in the running configuration file.
4. Add the Cisco device to Safeguard for Privileged Passwords using password authentication.

Preparing Dell iDRAC devices

Safeguard for Privileged Passwords supports the Dell Remote Access Controller that is integrated with Dell PowerEdge servers. Safeguard for Privileged Passwords uses the SSH protocol to connect to iDRAC devices.

To prepare an iDRAC device for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the iDRAC device using password authentication.

Preparing VMware ESXi hosts

Safeguard for Privileged Passwords supports VMware ESXi hosts.

IMPORTANT: Safeguard for Privileged Passwords can only manage local users on a VMware host.

To prepare a VMware ESXi host for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords:
    a. Specify the network address.
    b. Specify port 443 as the HTTPS port.

Preparing Fortinet FortiOS devices

Safeguard for Privileged Passwords supports Fortinet Internet appliances. Safeguard for Privileged Passwords uses the SSH protocol to connect to Fortinet devices.

To prepare a Fortinet FortiOS device for Safeguard for Privileged Passwords

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: Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords using password authentication.

Preparing F5 Big-IP devices

Safeguard for Privileged Passwords supports F5 Big-IP devices. Safeguard for Privileged Passwords uses the SSH protocol to connect to F5 Big-IP devices.

To prepare an F5 Big-IP device for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords using password or SSH key authentication.

Preparing HP iLO servers

In Safeguard for Privileged Passwords, the **HP iLO** operating system is an HP Integrated Lights-Out (iLO) HP Proliant server. Safeguard for Privileged Passwords connects to HP iLO systems using SSH. Password check and change is supported. Account discovery is not supported.

To prepare an HP iLO server for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the HP iLO server using password authentication.

Preparing HP iLO MP (Management Processors)

In Safeguard for Privileged Passwords the **HP iLO MP** operating system is an HP Integrity Integrated Lights-Out (iLO) Management Processor. Safeguard for Privileged Passwords connects to HP iLO MP systems using SSH.

To prepare an HP iLO Management Processor for Safeguard for Privileged Passwords

1. Create a service account with the Administer User Accounts privilege and assign it a password.
2. Verify that SSH is enabled.
3. In Safeguard for Privileged Passwords, create the asset and accounts for the HP iLO MP asset type using password authentication.

Preparing IBM i (AS/400) systems

Safeguard for Privileged Passwords supports IBM i (AS/400) systems.

To prepare IBM i systems for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the IBM iSeries (AS/400) system using password authentication.

About certificate support for the telnet protocol

Safeguard for Privileged Passwords automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, Safeguard for Privileged Passwords does not support client certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, Safeguard for Privileged Passwords cannot support that configuration.

Preparing JunOS Juniper Networks systems

Safeguard for Privileged Passwords uses the Juniper Networks JunOS operating system to manage Juniper Networks routers and switches. Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the Juniper Networks JunOS asset type using password authentication.

Preparing MongoDB

Safeguard for Privileged Passwords makes 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 Safeguard for Privileged Passwords.

To configure MongoDB for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, 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, Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords will fail.

Preparing MySQL servers

To prepare a MySQL server for Safeguard for Privileged Passwords, 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 Safeguard for Privileged Passwords. For more information, see Trusted Certificates on page 363.

For more information about how Safeguard for Privileged Passwords database servers use SSL, see How do Safeguard for Privileged Passwords database servers use SSL on page 571.

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:

- John : Permit John to log in from any host (default)
- John@%: Permit John to log in from any host
- John@10.1.%: Permit John to log in from any IP address in 10.1.xx

Preparing Oracle databases

To prepare an Oracle database for Safeguard for Privileged Passwords, 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 Safeguard for Privileged Passwords.

Preparing PAN-OS (Palo Alto) networks

In Safeguard for Privileged Passwords the PAN-OS operating system is used by Palo Alto Networks appliances. Safeguard for Privileged Passwords connects to PAN-OS systems using SSH.

To prepare a Palo Alto Networks system for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the Palo Alto Networks asset type using password authentication.

Preparing PostgreSQL

Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords.

To configure PostgreSQL for Safeguard for Privileged Passwords

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 PostgreSQL Security Guide for the appropriate settings for your organization.

2. Verify that you can log in with the service account.
3. In Safeguard for Privileged Passwords, 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.

   NOTE: When you create an account of Dialog User or Communication Data type, Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords will fail.

Preparing RACF mainframe systems

This applies to both RACF mainframe and RACF mainframe LDAP platforms.

To prepare IBM RACF mainframe systems for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the z/OS system using password authentication.

About certificate support for the telnet protocol

Safeguard for Privileged Passwords automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, Safeguard for Privileged Passwords does not support client certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, Safeguard for Privileged Passwords cannot support that configuration.

Preparing SAP HANA

Safeguard for Privileged Passwords makes 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 580.

To configure SAP HANA for Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the SAP asset type using password authentication. You must specify the **SAP Client ID** number as well as the **Port** used by the SAP instance.

   When you create an account of Dialog User or Communication Data type, Safeguard for Privileged Passwords 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 for Privileged Passwords will fail.

Preparing SAP Netweaver Application Servers

Safeguard for Privileged Passwords makes 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 580.

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 Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the SAP asset type using password authentication. You must specify the **SAP Client ID** number 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 Sybase (Adaptive Server Enterprise) servers

To prepare a Sybase ASE (Adaptive Server Enterprise) server for Safeguard for Privileged Passwords, refer to the documentation for your Sybase ASE 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 Safeguard for Privileged Passwords. For more information, see Trusted Certificates on page 363.

For more information about how Safeguard for Privileged Passwords database servers use SSL, see How do Safeguard for Privileged Passwords database servers use SSL on page 571.

Preparing SonicOS devices

Safeguard for Privileged Passwords supports SonicOS Internet appliances. Safeguard for Privileged Passwords uses the SSH protocol to connect to SonicOS devices.

To prepare a SonicOS device for Safeguard for Privileged Passwords

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: Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords using password authentication.

Preparing SonicWALL SMA or CMS appliances

Here are some important notes about configuring a SonicWALL SMA or CMS appliance for Safeguard for Privileged Passwords:

1. Use the local admin account as the service account.
2. Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords, 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 Safeguard for Privileged Passwords. For more information, see Trusted Certificates on page 363.

For more information about how Safeguard for Privileged Passwords database servers use SSL, see How do Safeguard for Privileged Passwords database servers use SSL on page 571.

To configure a SQL Server for Safeguard for Privileged Passwords (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 Safeguard for Privileged Passwords.

1. Log in to the Safeguard for Privileged Passwords desktop client as an Asset Administrator.
2. Navigate to **Administrative Tools** | **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 Safeguard for Privileged Passwords (with an authentication type of Directory Account)

NOTE: To mange 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 Safeguard for Privileged Passwords.

1. Add a directory and directory users.
   a. Log in as an Asset Administrator.
   b. Navigate to **Administrative Tools** | **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 215.

2. Add an SQL Server asset and account information.
    a. Log in to the Safeguard for Privileged Passwords desktop client as an Asset Administrator.
    b. From **Administrative Tools** | **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.

Preparing Top Secret mainframe systems

Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords

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 Safeguard for Privileged Passwords, create the asset and accounts for the z/OS system using password authentication.

About certificate support for the telnet protocol

Safeguard for Privileged Passwords automatically accepts any server certificate that the connection offers and does not verify the trust chain on the telnet certificate. In addition, Safeguard for Privileged Passwords does not support client certificate selection, so if telnet requires that the client present a certificate that is signed by a recognized authority, Safeguard for Privileged Passwords cannot support that configuration.

Preparing Unix-based systems

Safeguard for Privileged Passwords 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 for the service account. If you want to use an SSH key generated and configured by Safeguard for Privileged Passwords, 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
   - passwd

   AIX:

   - sed
   - grep
   - passwd
   - pwdadm

   Mac OS X

   - 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

Safeguard for Privileged Passwords supports Windows systems.

OpenSSH on Windows 7 and 8

The OpenSSH port on Windows 7 and 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 reduce the CommandTimeout when running TestConnection, ChangePassword and CheckPassword.

To prepare Windows systems for Safeguard for Privileged Passwords

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 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 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 to allow changing account passwords. For more information, see Minimum required permissions for Windows assets on page 536.
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.

- When possible, RPC ephemeral ports should also be accessible. For more information, see Service overview and network port requirements for Windows.

5. Change the local security policy:

   Before Safeguard for Privileged Passwords 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 fails on page 540.

For additional information on ports, see Safeguard ports.

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).

Asset password management

Using a local account or domain account:

- 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)

Preparing Windows SSH systems

Safeguard for Privileged Passwords supports Windows SSH systems. Windows SSH uses port 22 on the platform.

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.
3. Ensure the service account is added to the local Administrator's group to allow change password permissions.

26

Troubleshooting

One Identity recommends the following resolutions to some of the common problems you may encounter as you deploy and use Safeguard for Privileged Passwords. For more information about how to troubleshoot Safeguard for Privileged Passwords, refer to the Appliance settings.

- Anti-CSRF (cross-site request forgery) token error
- Connectivity failures
- Cannot connect to remote machine through SSH or RDP
- Cannot delete account
- Cannot play session message
- Domain user denied access to Safeguard for Privileged Passwords
- LCD status messages
- My Mac keychain password was lost
- Password fails for Unix host
- Password is pending review
- Password is pending a reset
- Profile did not run
- Recovery Kiosk (Serial Kiosk)
- Replica not adding
- System services did not update or restart after password change
- Test Connection failures
- Timeout errors causing operations to fail
- User locked out
- User not notified

Related Topics

Frequently asked questions

Anti-CSRF (cross-site request forgery) token error

Cross-site request forgery (CSRF) occurs when unauthorized commands are transmitted from a user that the web application trusts. Anti-CSRF is a type of CSRF protection. It is a random string that is only known by the user's browser and the web application

If you receive an *Anti Cross-Site Request Forgery token error* when attempting to log in to Safeguard for Privileged Passwords using Microsoft Internet Explorer 9 on Windows 7 SP1, this indicates that cookies are blocked.

To resolve this issue

1. In Internet Explorer, open **Tools** and choose **Internet Options**.
2. In the **Privacy** tab, click the **Advanced** button.
3. Select the **Always allow session cookies** option.

Connectivity failures

The most common causes of failure in Safeguard for Privileged Passwords 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 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 fails

A local account password 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 Safeguard for Privileged Passwords 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 535.

Incorrect authentication credentials

You must have the correct user name and password to authenticate to an asset.

To resolve incorrect service account credentials

1. Verify the service account credentials match the credentials in Safeguard for Privileged Passwords asset information (**Administrative Tools** | **Assets** | **Connection**). For more information, see About service accounts on page 201.
2. Perform **Test Connection** to verify connection. For more information, see About Test Connection on page 202.
3. Attempt to check, change, and set password again. For more information, see Checking, changing, or setting an account password on page 165.

Missing or incorrect SSH host key

If a Safeguard for Privileged Passwords asset requires an SSH host key and does not have one, Safeguard for Privileged Passwords will not be able to communicate with the asset. For more information, see Certificate issue on page 556.

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 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

Safeguard for Privileged Passwords uses the following host key algorithms for key exchange:

- DSA
- ECDSA
- RSA

To correct a mismatched SSH host key, run **Test Connection**.

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 556.

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 201.

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 again on the account that failed.

If the asset is running a Windows operating system, a local account password 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 Safeguard for Privileged Passwords can change 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 **Run all administrators in Admin Approval Mode** option. For more information, see Change password fails on page 540.

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 Safeguard for Privileged Passwords desktop 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 Safeguard for Privileged Passwords is trying to change the password 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 for this account, Safeguard displays the password that was manually set. However, when the requester attempts to log in to the asset using the bad account and password, 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 Safeguard for Privileged Passwords.

Workaround: To delete the account with the misspelled name, first manually set the password on the account. Once the account password is reset, Safeguard for Privileged Passwords will allow you to delete the account.

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 Safeguard for Privileged Passwords

If you add a directory user who has the `User must change password at next logon` option enabled in Active Directory, Safeguard for Privileged Passwords prevents that user from logging in. There are two ways to allow the directory user to log in to Safeguard for Privileged Passwords successfully:

- Have the directory user use his domain account to log in to an asset joined to Active Directory. When prompted he can change his 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 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 Safeguard for Privileged Passwords, 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 Safeguard for Privileged Passwords 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 575.
- **Starting core**: Indicates that Safeguard for Privileged Passwords is being loaded.
- **Starting database**: Indicates that the Safeguard for Privileged Passwords database is being loaded.
- **Starting reboot**: Indicates the appliance is being rebooted.
- **Starting services**: Indicates that Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 208: 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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>

My Mac keychain password was lost

The keychain in Macintosh OS X is the Apple password management system. A keychain can store all your passwords 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 Safeguard for Privileged Passwords, you may receive a message that says, `The system was unable to unlock your login keychain`. That is because Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords. This causes the following issues:

- Check Password for that account will fail. When Safeguard for Privileged Passwords compares the password on the Unix host with the password in Safeguard for Privileged Passwords, they never match because the Unix host truncated the password generated by Safeguard for Privileged Passwords.

- A user will not be able to log in to the Unix host account successfully with the password provided by Safeguard for Privileged Passwords unless they truncate the password to the allowable length imposed by the operating system.

Password is pending review

Safeguard for Privileged Passwords can resolve a situation when a user needs to request an account password but cannot because there is a previous password release request still in the Pending Review state and the designated reviewer is not available. If the request is left in this state, Safeguard for Privileged Passwords prevents users from checking out the account password. In such a situation, the Security Policy Administrator can close the request without review.

You can also set up requests so that pending reviews do not block access. For more information, see Reviewer tab on page 282.

To close a password without review

1. Log in as a user with Security Policy Administrator permissions.
2. On the **Home** page, click **Refresh**.
3. Open **Administrator** to review the pending request.
4. Select **Close Request**.

5. Type an explanation in the **Comment** box of up to 255 characters (required).
6. Select **Close Request**.

You can query and view all requests closed without review in the **Activity Center**. Filter the events by **Password Request Closed**, then export the search results to see the old state and new state.

Related Topics

Password is pending a reset

Password is pending a reset

If a user receives a persistent message that states either of the following, the account password is stuck in a pending password change state:

- `You cannot checkout the password for this account while another request is pending password reset`
- `This account has password 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. For more information, see Checking, changing, or setting an account password on page 165.
- 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 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 Reviewer tab on page 282.

Related Topics

Password is pending review

Profile did not run

The password management settings **Settings** | **Access Request** | **Enable or Disable Services** enable the automatic profile check and change schedules in partitions.

Ensure the password management settings are enable for profiles to run on schedule:

- Check Password Management Enabled
- Change Password Management Enabled

For more information, see Enable or Disable Services (Access and management services) on page 309.

Recovery Kiosk (Serial Kiosk)

Safeguard for Privileged Passwords provides a Recovery Kiosk (Serial Kiosk) with the following options.

- Appliance information (Recovery Kiosk): Allows you to view basic appliance information.
- 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 66.

  > **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. 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 68.**
  >
  > **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 you are using version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, you appliance will reset down to 6.0 LTS and you will have to patch up to your current version. For more information, see Long Term Support (LTS) and Feature Releases on page 46.**

- 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**
   - **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

Safeguard for Privileged Passwords provides these keyboard shortcuts. If you make the window too small to accommodate the kiosk elements, Safeguard for Privileged Passwords tells you how to readjust the window size.

- **Ctrl + D**: Resets the kiosk to its original state. Clears challenges and options.

  CAUTION: When resetting the Bootstrap Administrator's password or performing a factory reset, if you reset the kiosk *before* you receive the response from One Identity Support, you must submit a new challenge.

- **Ctrl + R**: Re-fdraws 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 for AWS or 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 (X0), 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.

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 Safeguard for Privileged PasswordsWindows desktop client, 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 Safeguard for Privileged Passwords Windows desktop client, 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 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 Safeguard for Privileged Passwords for a set number of days, Safeguard for Privileged Passwords disables the user account. This is set using the **Disable After** setting in **Administrative Tools** | **Settings** | **Safeguard for Privileged Passwords Access** | **Login Control**.

To reset the Bootstrap Administrator's password

1. From the Recovery Kiosk, select the **Admin Password Reset** option.
2. Press the right arrow.
3. At **id**, enter your identification and press the **Tab** key (or down arrow).
4. At **Get Challenge**, press the **Enter** key.

   Safeguard for Privileged Passwords produces a challenge.
5. Copy and paste the challenge and send it to One Identity Support.
6. When you get the response from One Identity Support, copy and paste the response

into the kiosk screen and select **Reset Password**.

- A challenge response is only good for 48 hours.
- Do not navigate away from the page or refresh during a challenge response operation. Doing so will invalidate the challenge response.

One Identity Support resets the Bootstrap Administrator's password back to **Admin123**.

NOTE: **Best practice**: To keep your appliance secure, change the default password for the Bootstrap Administrator's account.

Factory reset from the Recovery Kiosk

There is a **Factory Reset** selection in the Recovery Kiosk. **Factory Reset** allows you to reset a Safeguard for Privileged Passwords 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. 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 68.

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 you are using version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, you appliance will reset down to 6.0 LTS and you will have to patch up to your current version. For more information, see Long Term Support (LTS) and Feature Releases on page 46.

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 68.

To perform a factory reset from the Recovery Kiosk

1. To perform a hardware factory reset, go to the Recovery Kiosk. For more information, see Recovery Kiosk (Serial Kiosk) on page 549.
2. Select **Factory Reset**.

3. Press the right arrow.
4. At **id**, enter your email or name and press the **Tab** key (or down arrow).
5. At **Get Challenge**, press the **Enter** key. Safeguard for Privileged Passwords produces a challenge.
6. Copy and paste the challenge and send it to One Identity Support.
   - A challenge response is only good for 48 hours.
   - Do not navigate away from the page or refresh during a challenge response operation. Doing so will invalidate the challenge response.
7. When you get the response from One Identity Support, copy and paste the response into the kiosk screen and select **Factory Reset**.

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 Safeguard for Privileged Passwords as the primary. All members of a cluster must be the same.

System services did not update or restart after password change

If the system services do not update or restart after an automatic password 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** tab of the profile that governs the service account. For more information, see Creating a profile on page 302.

For service accounts that run system services or scheduled system tasks, verify the options on the profile's **Change password** tab that enable or disable automatic service update, or restart. You must update the Change Password Setting to change these options. For more information, see Change Password on page 425.

Test Connection failures

The most common causes of failure in Safeguard for Privileged Passwords are either connectivity issues between the appliance and the managed system, or problems with service accounts.For more information, see Connectivity failures on page 540.

Disabling User Account Control (UAC) Admin Approval Mode on a remote host can also resolve **Test Connection** failures. For more information, see Change password fails on page 540.

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 Safeguard for Privileged Passwords's cipher support.
- Domain controller issue: Learn how Safeguard for Privileged Passwords manages passwords for accounts on domain controllers.
- Networking issue: Learn how to resolve system connectivity issues.
- Windows WMI connection: Learn how to enable Safeguard for Privileged Passwords 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**, Safeguard for Privileged Passwords 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 Certificates store in Safeguard for Privileged Passwords.
- 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 541.

Cipher support

Both the Safeguard for Privileged Passwords 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, Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords to the list of ciphers.

Safeguard for Privileged Passwords 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

Safeguard for Privileged Passwords does not manage passwords for accounts on domain controllers; Safeguard for Privileged Passwords 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 156.

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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords.

> 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 Safeguard for Privileged Passwords for a set number of days, Safeguard for Privileged Passwords disables the user account.

> NOTE: This is set using the **Disable After** setting in **Administrative Tools** | **Settings** | **Password Settings** | **Login Control**. For more information, see Login Control on page 436.

Related Topics

Unlocking a 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 Safeguard for Privileged Passwords correctly for the email notifications to work properly. For more information, see Enabling email notifications on page 396.

Notification lists

Safeguard for Privileged Passwords does not dynamically maintain the email addresses for an escalation notification contact list.

If you change a Safeguard for Privileged Passwords user's email address or delete a Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords, the user will still receive the notification.

27

Frequently asked questions

The following topics will help you find answers to some of your questions about managing Safeguard for Privileged Passwords:

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 Safeguard for Privileged Passwords messages when making RDP connections

How do I set up telnet and TN3270/TN5250 session access requests

How do I set the appliance system time

How do Safeguard for Privileged Passwords 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

Verifying syslog server configuration

Why did the password change during an open request

Related Topics

Appliance settings

Troubleshooting

How do I audit transaction activity

The appliance records all activities performed within 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 507.

Safeguard for Privileged Passwords provides 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 166.
- Check and Change Log: Where you view an account's password validation and reset history. Access the **Check and Change Log** from **Accounts**. For more information, see Accounts on page 147.
- History: Where you view the details of each operation that has affected the selected item.Each of the **Administrative Tools** has a History tab. For more information, see History tab (account) on page 154.
- Activity Center: Where you can search for and review any activity for a specific time frame. For more information, see Activity Center on page 94.
- Workflow: 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 102.
- 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 104.

How do I configure external federation authentication

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 Safeguard for Privileged Passwords user account to be associated with the federated account.

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. This works in both a web browser and the Safeguard desktop client application.
  IMPORTANT: For on-prem VM (Hyper-V or VMware only: After installing v6.0 or after a backup restore from v6.0, the log on to an existing External Federation provider will fail. See KB Article xxxx to for the steps to edit the app registration’s Application ID URI.
- 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, IdP initiated logins only work in the web browser, not the Safeguard desktop client application.

NOTE: Additional two-factor authentication can be assigned to the associated Safeguard for Privileged Passwords user account to force the user to authenticate again after being redirected back from the external STS.

To use external federation, you must first download the federation metadata XML for your STS and save it to a file. For example, for Microsoft's AD FS, you can download the federation metadata XML from:

https://<adfs server>/FederationMetadata/2007-06/FederationMetadata.xml.

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 Safeguard for Privileged Passwords.

To add an external federation service provider

1. In Settings, select **External Integration** | **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. A case-insensitive comparison will be used on this value when performing Home Realm Discovery.

      Wildcards are not allowed.

      Limit: 255 characters

   c. **Federation Metadata File**: Choose or enter the file path to the STS federation metadata file that you previously downloaded.

   d. **Download Safeguard for Privileged Passwords Federation Metadata**: If you have not done so before, click the link to download a copy of Safeguard for Privileged Passwords'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.

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 Safeguard for Privileged Passwords's federation metadata by clicking the link when you entered the STS information in Safeguard for Privileged Passwords. You can also download the Safeguard for Privileged Passwords federation metadata at any time using one of the following methods:

- Click **Settings** | **External Integration** | **Identity and Authentication**. Click **Download Safeguard Federation Metadata**.
- Download the file from the following URL:

  https://<Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords federation metadata XML file you downloaded.

- The App ID for Safeguard for Privileged Passwords 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.

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 must update the metadata in Safeguard for Privileged Passwords by uploading a new copy of your STS's metadata file. Safeguard for Privileged Passwords will not automatically attempt to refresh the metadata.

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 Safeguard for Privileged Passwords: KB Article 233669
- Configuring Microsoft's Azure AD for Safeguard for Privileged Passwords: KB Article 233671

How do I add an external federation user account

It is the responsibility of either the Authorizer Administrator or the User Administrator to add an associated external federation Safeguard for Privileged Passwords user.

Preparation

You must add external federation service providers to Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords if you need it.

To add a user

1. Navigate to **Administrative Tools** | **Users**.
2. In **Users**, click **+ Add 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.
    - Location tab (add user): Where you set the user's time zone.
    - Permissions tab (add user): Where you set the user's administrator permissions.

How do I manage accounts on unsupported platforms

Safeguard for Privileged Passwords makes it possible for you to manage passwords for accounts on unsupported platforms and not addressed by a Custom platforms.

You will use a profile with a manual change password setting.

For example, you may have an asset that is not on the network. The manual change password setting allows you to comply with your company policies to change account passwords on a regular schedule without using the Safeguard for Privileged Passwords automatic change password settings. Safeguard for Privileged Passwords notifies you by email, toast notification, or both on a set schedule to change account passwords manually. You can then reset the password yourself, or allow Safeguard for Privileged Passwords to generate a random password according to the password rule selected in the profile.

> IMPORTANT: After you change the password in Safeguard for Privileged Passwords you must remember to change the password on the account; Safeguard for Privileged Passwords does not do that automatically for you.

The following summarizes the general workflow for managing accounts on unsupported platforms.

To manage account passwords manually

1. Configure a profile with a manual change password setting and assign asset accounts to it. For more information, see Adding change password settings on page 426.
2. Ensure toast notifications or email notifications are properly configured. For more information, see Settings (desktop client) or Enabling email notifications.
3. When notified to change an account password, choose the **Set Password** option you prefer:
   a. **Generate Password:** To have Safeguard for Privileged Passwords generate a new random password , that complies with the password rule that is set in the account's profile.
      i. Click **Generate Password** to display the **Password Change** dialog.
      ii. Click **Show Password** to reveal the new password.
      iii. Click **Copy** to place the value into your copy buffer.
         - Log in to your device, using the old password, and change it to the value in your copy buffer.
      iv. Click **Success** to change the password in the Safeguard for Privileged Passwords database.
   b. **Manual Password**: To manually set the account password in the Safeguard for Privileged Passwords database.
      i. Click **Manual Password** to display the **Set Password** dialog.
      ii. Enter and save a new password.

      OK updates the Safeguard for Privileged Passwords database.
      iii. Set the account password on the physical device to synchronize it with Safeguard for Privileged Passwords.

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 *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 Safeguard for Privileged Passwords web client using the Appliance Administrator account.
2. Click **Settings** to go to the **Settings: Appliance** page.
3. Click **Networking** to configure the appliance. For more information, see Networking on page 326.
   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 330.
   d. Click **Save**.

(desktop client) To modify the appliance configuration settings

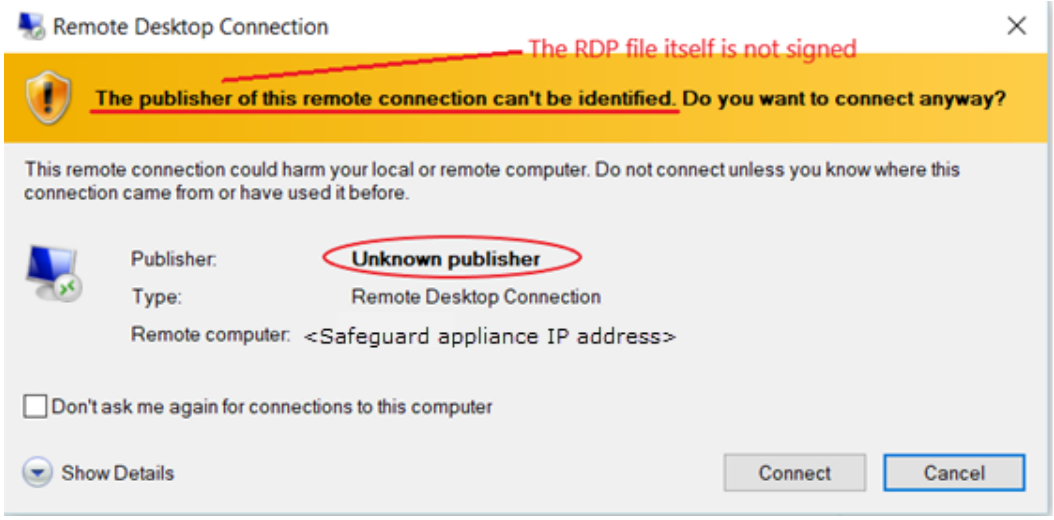
1. Log in using the Appliance Administrator account.
2. Navigate to **Administrative Tools** | **Settings** | **Appliance**.
3. Expand the **Time** pane to enable NTP and set the primary and secondary NTP servers. Click **OK**. For more information, see Time on page 330.
4. Expand the **Appliance Information** pane to change the appliance name.
   1. To change the appliance's name, click **Edit** next to the **Appliance Name**.
5. Expand the **Networking** pane to add or modify DSN suffixes. For more information, see Networking on page 326.

a. To change the DNS suffixes for your primary interface, click ✎**Edit** next to the **Network Interface X0** heading.
   - Enter the DSN suffixes to be used.
   - Click **OK**.

How do I prevent Safeguard for Privileged Passwords messages when making RDP connections

When making an RDP connection, you may encounter two different certificate messages.

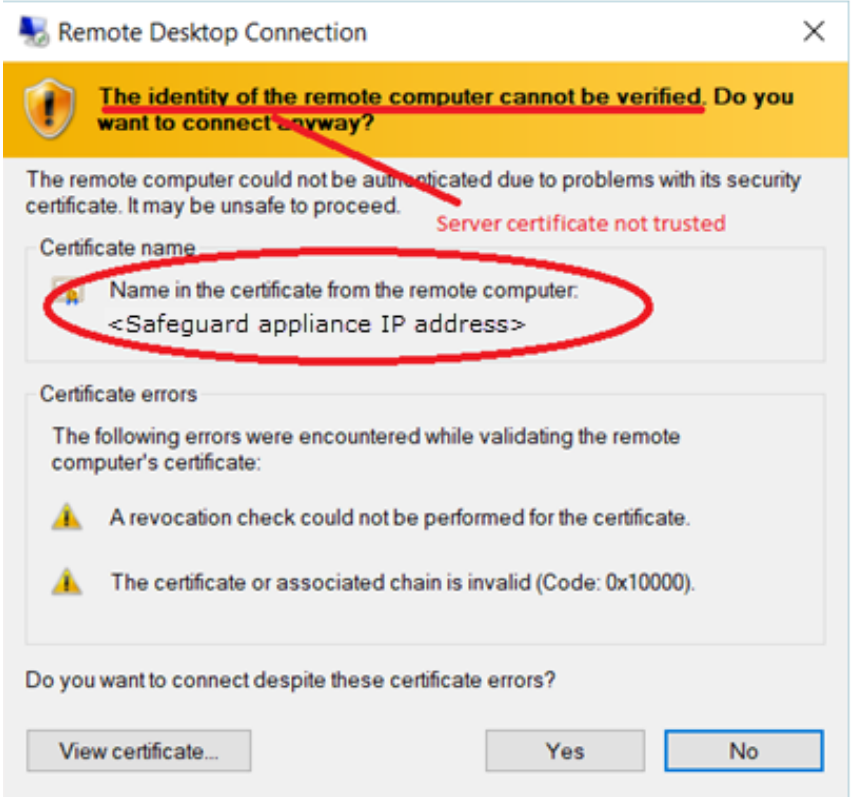
- Unsigned RDP file message



  This message occurs when Remote Desktop Connection opens the RDP file that is downloaded when you click ▶ **Play** in the Safeguard for Privileged Passwords user interface.

  We are currently working on a solution that will allow Safeguard for Privileged Passwords to sign this RDP file to avoid this message.

- Untrusted server certification message



This message occurs when the workstation has not trusted the Safeguard for Privileged Passwords 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

Safeguard for Privileged Passwords (SPP) supports session access requests with mainframes using software terminal emulation including telnet and TN3270/TN5250 over telnet. Safeguard for Privileged Sessions (SPS) 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 Safeguard for Privileged Passwords and all required log in information is available through Safeguard for Privileged Passwords.

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.

SPS 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 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 SPS 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 Safeguard for Privileged Passwords (SPP).

- The Asset Administrator adds the mainframe asset including the **Telnet Session Port** that is identified on the **Administrative Tools** | **Asset** | **Management** tab. For more information, see Adding an asset on page 193.
- The Security Policy Administrator sets the **Access Type** (**Telnet**) on the **Administrative Tools** | **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. 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 SPS 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** to complete the password 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 I set the appliance system time

As a best practice, set an NTP server to eliminate possible time-related issues. For more information, see Time.

> **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.**

To set the time on your appliance

- Use the appliance API to change the appliance time (SystemTime). For information about using the API, see Using the API.

How do Safeguard for Privileged Passwords database servers use SSL

Some database servers use Secure Socket Layer (SSL) when communicating with Safeguard for Privileged Passwords. 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. Safeguard for Privileged Passwords installs the appropriate software driver on the appliance to communicate with the platform. The configuration data that Safeguard for Privileged Passwords 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 Server is 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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords 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 209: Microsoft SQL Server SSL support

Safeguard for Privileged Passwords 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	Safeguard for Privileged Passwords requests that the SQL server encrypt the session using a generated self-signed certificate.
Yes	No	n/a	Yes	Safeguard for Privileged Passwords

				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	Safeguard for Privileged Passwords requests that the SQL server encrypt the session and verify the server certificate against the trusted CA certificates in Safeguard for Privileged Passwords.

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 Safeguard for Privileged Passwords 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 Safeguard for Privileged Passwords client does not request it. However, the Safeguard for Privileged Passwords client cannot request to use SSL just for encryption; it can only request SSL if you have imported the correct CA certificate to Safeguard for Privileged Passwords.

NOTE: It is possible to detect that SSL is in use from within a session by examining the session variables. That is, the Safeguard for Privileged Passwords client can detect if a request to use SSL has not been honored and displays an error.

Table 210: MySQL Server SSL support

Safeguard for Privileged Passwords 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

Safeguard for Privileged Passwords Use SSL Encryption Option	SSL Supported on MySQL Server	Result
		requires it for this user.
Yes	No	Safeguard for Privileged Passwords client detects this and reports a failure.
Yes	Yes	Safeguard for Privileged Passwords requests that the MySQL server encrypt the session and verity the server certificate against the trusted CA certificate in Safeguard for Privileged Passwords

For more information, see Preparing MySQL servers on page 526.

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 Safeguard for Privileged Passwords client to a particular port.

The Safeguard for Privileged Passwords client cannot request to use SSL just for encryption; it can only request SSL if you have imported the correct CA certificate to Safeguard for Privileged Passwords.

Table 211: Sybase ASE Server SSL support

Safeguard for Privileged Passwords 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.
Yes	Yes	Safeguard for Privileged Passwords requests that the Sybase server encrypt the session and verify the server certificate against the trusted CA certificates in Safeguard for Privileged Passwords.

For more information, see Preparing Sybase (Adaptive Server Enterprise) servers on page 530.

What are the access request states

Safeguard for Privileged Passwords uses the following access request states, which change as a request steps through the workflow process.

Table 212: Access request states

State	Description
Available	Approved requests that are ready for the requester. That is, for password release requests, the requester can view or copy the password. 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

Safeguard for Privileged Passwords hardware and virtual 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. For more information, see Backup and Retention settings on page 343. The appliance (at least one appliance in a clustered environment), should be set up to take a scheduled backup regularly, that should be saved to an archive server so that if something happens, you can recover with minimum downtime and loss.

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 549.
   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**.
   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.
   a. 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 Safeguard for Privileged Passwords to start.
   b. If you log into the appliance using the desktop client while Safeguard for Privileged Passwords is starting, you will see a Maintenance mode screen. At the end of the Maintenance mode, you will see a **Restart Desktop Client** button or the Quarantine warning.
      i. If you see the **Restart Desktop Client** button, the restart successfully recovered the appliance and brought the appliance back in a healthy state.
      ii. If the Quarantine warning appears, 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 491.

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 483.
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 497.

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. 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 68.**
>
> **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 you are using version 6.6 (feature release) or 6.0.6 LTS (maintenance Long Term Support release) and then factory reset, you appliance will reset down to 6.0 LTS and you will have to patch up to your current version. For more information, see Long Term Support (LTS) and Feature Releases on page 46.**

One Identity Technical Support can determine if a factory reset is necessary. If a factory reset is the last option, you will need to 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 553.

   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. Re-apply any patches you had installed.
   c. If this is an unclustered appliance, upload and restore the most recent backup to retrieve your data. For more information, see Restore on page 353.
   d. If the appliance was a member of a cluster, skip the restore step and join the appliance to the cluster as if it were a brand new appliance. For more information, see Enrolling replicas into a cluster on page 482.Safeguard for Privileged Passwords 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

Verifying syslog server configuration

Use the **Send Test Event** link located below the Syslog configuration table on the **Syslog** pane to verify your syslog server configuration. Navigate to **Administrative Tools** | **Settings** | **External Integration** | **Syslog**.

To validate your setup

1. When configuring your syslog server, on the **Syslog** dialog add the test event.
2. Back on the **Syslog** pane, select the syslog server configuration from the table, then select **Send Test Event**.

   Safeguard for Privileged Passwords logs a test message to the designated syslog server.

NOTE: To log event messages to a syslog server, you must configure Safeguard for Privileged Passwords to send alerts. For more information, see Configuring alerts on page 118.

Why did the password change during an open request

There are three ways a password can change while a user has it checked out.

1. An Asset Administrator manually changes the password. For more information, see Checking, changing, or setting an account password on page 165.

2. A profile was scheduled to automatically change the password. For more information, see Change Password on page 425.
3. A policy allows both simultaneous access and requires that the password change when a user checks it in.

If the password changes while a user has it checked out, and the current request is still valid, the user can select either **Copy** or **Show Password** again to obtain the new password.

Appendix A

Safeguard ports

Safeguard for Privileged Passwords requires port availability for various system operations.

Port details

Safeguard network port details are in the following table.

Table 213: 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	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	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

Use in SPP	Appliance port	Protocol	Description
			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. 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 check and change)	445	TCP SMB	NetLogon Service (NP-In) is used to perform password check and changes for Windows Active Directory and 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 (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

Use in SPP	Appliance port	Protocol	Description
			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 joined with SPP.
			• SPS to SPP:
			  • SPS completes the join by talking to SPP on port 8649.
			  • SPS authenticates a new session and acquires the password from SPP by 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.

Use in SPP	Appliance port	Protocol	Description
			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	TCP / UDP (X0)	TINC (655) is open for secure VPN communication between appliances in a clustered high-availability configuration. TINC perfers UDP and uses TCP if UDP is unreliable. See KB article 232671. To enroll an appliance into a cluster, the appliance must communicate over port 655 UDP/TCP and port 443 TCP, and must have IPv4 or IPv6 network addresses (not mixed). See: • KB article 232289 • KB article 252260 • KB article 232671 • Cluster settings • 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. To enroll an appliance into a cluster, the appliance must communicate over port 655 UDP/TCP and port 443 TCP, and must have IPv4 or IPv6 network addresses (not mixed). 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

Use in SPP	Appliance port	Protocol	Description
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 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

Other 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

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 Workflow

Approval Anywhere - 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 2.7 or later migration guidance

Safeguard for Privileged Passwords version 2.7 was simplified to allow for a separation of duties based only on identity management, asset management, access policy configuration, and appliance maintenance. In the migration to version 2.7 or later, greater flexibility is realized through these high-level assignments:

- Directories are migrated to assets.
- Accounts include both directory accounts and asset accounts.
- Each directory is assigned its own partition in the migration to version 2.7 or later.

The following information details the changes from version 2.6 to version 2.7 or later. The same information is generally true if you are upgrading from version 2.1 forward to version 2.7 or later.

Before you migrate

- Make sure you back up before migrating to version 2.7 or later.
- Be sure you have data you want to migrate and perform general clean up. For example, if you have entities that are not needed, remove them before migrating.
- Complete as many outstanding Access Requests as possible. This is especially important for Active Directory Access Requests because any outstanding Active Directory Access Requests will need to be recreated after the migration since they cannot be resubmitted.
- Save all necessary version 2.6 logs. Directory log history prior to the migration to version 2.7 or later is not available after the migration. Details follow.
    - Before the migration to version 2.7 or later, Directory Administrators, Asset Administrators, and Auditors can see audit log history for each of the directories, regardless of who created or changed them.
    - The migration takes Directories and turns them into directory assets. All associated relationships with directories are also migrated to the new directory assets. The Directory Administrator role is removed and users with Directory Administrator permission are assigned as a partition owners for directories that are migrated to assets.

    - After the migration to version 2.7 or later, the Asset Administrator can see the directory asset whose audit log history starts on the day of the migration. Events prior to migration are not available.
- We recommend two clients:
    - A version 2.6 client to connect to older appliances
    - A new version 2.7 or later client to get the new features of Directory Assets and Discovery

      This recommendation is made because a new client uses v3 endpoints. A version 2.6 appliance doesn't know how to respond to v3 calls. An new client pointed to an old appliance will get an error when trying to connect. You will see this message: `The Safeguard desktop application is not compatible with this appliance. Please contact your administrator.`

What to expect

The following lists entity changes you will note in the migration to version 2.7. or later.

Directories are migrated to Assets

- Directories are migrated to assets with the appropriate platform assignment.
- Directories are still synced with Safeguard.
- Migrated directory assets reflect any account dependencies with Windows services and task on other assets.
- You can select whether a directory asset manages the forest or a subset of the forest. Multiple assets can be assigned against the same forest.
- Every migrated directory has **Managed Forest** selected so the administrator can create a directory to manage a domain or part of a domain. As assets, directories can be shared and all domains in a forest can be managed from one instance of a domain. Navigate to **Administrative Tools** | **Asset** | **Management** tab | **Managed Forest** check box.
- Every migrated directory asset has **Available for discovery across all partitions** selected so the asset is available for asset and account aiscovery jobs beyond partition boundaries. Any partition that exists is able to use this directory asset. Navigation: **Administrative Tools** | **Asset** | **Management** tab | **Available for discovery across all partitions** check box.
- Discovery detail grids will identify migrated directory assets with a **Partition** value of **Import**.
- Each migrated directory asset is assigned to its own partition and includes the Account Discovery jobs, the check and change schedules, account password rules, password sync groups, and related functions.
    - To view the Account Discovery job assigned as the results of migration, navigate to **Administrative Tools** | **Asset**. Select the directory asset then **Edit**. Then navigate to | **Account Discovery** tab to see the selected Account

Discovery job for the partition. If no schdule is selected, this message displays: `No Account Discovery Chosen`.

- Directory tags are migrated into the appropriate partition tag. To copy a tag to a new partition, change the description then copy the tag.

Administrative Tools | Directories removed and Discovery added

When Safeguard for Privileged Sessions version 2.7 is installed, directories, discovery jobs, and other related entities automatically migrate to the appropriate associations. The **Administrative Tools | Directories** selection is gone, and **Administrative Tools | Discovery** has been added. Functionality is reorganized and streamlined for better data control.

Discovery

- During migration, existing partition account discovery jobs are separated by platform type, for example, Unix, Windows, or Directory. As a result, you will see discovery jobs with the same name and a different prefix which denotes the platform. For example, you may see:
  - (Unix) AD-Asset Discovery account discovery job
  - (Windows) AD-Asset Discovery account discovery job

  Each discovery job is assigned the appropriate asset and settings that apply to the platform.

  You can rename or delete jobs, as needed. Navigate to: **Administrative Tools** | **Discovery**.
- In version 2.6, you can have several directory account discovery jobs assigned to the same directory. During migration, all the directory account discovery jobs assigned to a directory are put in a single account discovery job with multiple rules, one for each prior job. The job schedule follows the directory sync interval.
- In version 2.7, you can assign a profile to the account or a sync group using the account template in the Account Discovery job rule. For more information, see Adding an Account Discovery rule on page 254.

Account changes

- Accounts include directory accounts and asset accounts.
- Directory accounts are migrated into accounts and are assigned to the appropriate asset.
- Accounts identify the dependent assets.
- Every migrated account has **Available for use across all partitions** selected. For example, if you create an asset service account with this check box selected, the service account could be used from anywhere.

  Navigate to **Administrative Tools** | **Account** | **Management** tab | **Available for use across all partitions** check box.

- You cannot add the same account to multiple partitions from the same domain.
- You can select a directory account and view the assets that have dependency on the directory account.

  Navigate to **Administrative Tools** | **Accounts** | **Dependent Assets**.

Dynamic account group changes

The rules for dynamic asset groups and dynamic account groups include attributes for directory assets.

> NOTE: Dynamic asset groups rule attributes do not include attributes for directory accounts. A directory cannot be the target of an asset group because you can not get an RDP or SSH session to them. Dynamic asset groups are for Security Policy Administrator control and directories are not included in policies.

Identity and authentication provider migration

A directory identity provider is managed by creating a directory asset which points to the same directory. The directory identity provider can be created and, optionally, put under management or not.

During migration from earlier versions of Safeguard for Privileged Passwords, if there are Active Directory users and user groups, SPP determines if Active Directory should be the identity provider or not. To see the result of the migration:

1. Navigate to **Administrative Tools** | **Settings**.
2. Select the directory then the **General** tab.
3. Scroll down to **Available Domains for Identity and Authentication** to view the domains selected for the directory. Directory groups require the forest root domain to be visible and available for identity and authentication set on **Administrative Tools** | **Settings** | **External Integration** | **Identity and Authentication**. For more information, see Available Domains for Identity and Authentication (for Active Directory) on page 404.

After the initial migration to version 2.6, add the identity provider.

Entitlements and access request policies

- Entitlement access request policies are migrated. If the access configuration for the asset-based session asset is a directory and you are using the version 2.6 desktop client, the name of the directory account may be blank since version 2.6 understood only one assignment and version 2.7 or later handles multiple assignments. To verify this, navigate to the **Entitlements** | **Access Request Policy** | **Access Config** tab. For directory accounts, the **Asset-Based Session Access** is correctly identified as a **Directory Account**, however, the directory account name is blank.

Management

Directories can be subdivided so administrators can be assigned to manage portions of a directory. For example, Admin A may only manage objects in the Finance organizational

unit (OU) of the directory, and Admin B may only manage objects in the Engineering OU of the directory. This is possible via the settings on Assets including the asset **Name**, **Domain Name**, and whether to **Manage Forest**. This way, multiple assets can govern the same domain.

Directory accounts can be service accounts to other assets to run windows services/tasks on assets to keep password changes in sync.

Administrator role changes

- The Directory Administrator role is removed, and users with Directory Administrator permission are assigned as partition owners for directories that are migrated to assets. This role does not include the ability to manage identity providers.
- An Authorizer Administrator can now add an Active Directory forest only for identity to use as an unprivileged service account for connection.
- An Asset Administrator can now:
  - Use service accounts to manage Active Directory. The service accounts can have limited permissions within a single domain.
  - Use multiple service accounts for managing the same Active Directory domain with different limited permissions within the domain. For example, the administrator can add the domain as a managed asset multiple times with different service accounts.
  - Use a service account from Active Directory to manage an asset from a different partition so that the administrator does not have to add that Active Directory to each of the administrator's partitions.
  - Set up a dependent system for a service running as an Active Directory account that isn't in the administrator's partition. This avoids having to add the Active Directory asset or the account to the partition.
  - Add Active Directory for authentication to Safeguard for Privileged Passwords without managing any of the accounts in Active Directory.
  - Set up multiple assets for the same domain.

Appendix C

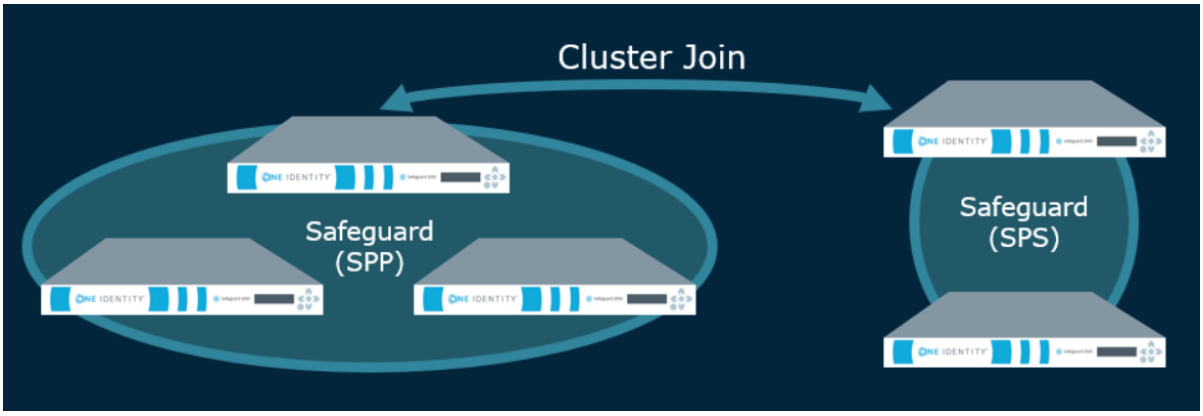
SPP and SPS sessions appliance join guidance

Safeguard for Privileged Passwords version 2.7 introduced the ability to join Safeguard for Privileged Sessions for session recording and auditing.

The Asset Administrator can join a Safeguard for Privileged Sessions (SPS) cluster to a Safeguard for Privileged Password (SPP) cluster of one appliance or more for session recording and auditing. The actual join must be between the SPP primary and the SPS cluster master. This means that the Safeguard for Privileged Sessions (SPS) cluster is aware of each node in an SPP cluster and vice-versa.

Once joined, all sessions are initiated by the SPP appliance via an access request and managed by the SPS appliance and sessions are recorded via the Sessions Appliance.

NOTE: If you have a single node SPS 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 SPS appliance in the cluster that is capable of recording sessions. See the *SPS Administration Guide*, Managing Safeguard for Privileged Sessions (SPS) clusters.



Additional overview information can be found in the *Safeguard for Privileged Sessions Administration Guide*, Passwords-initiated (SPP-initiated) workflow.

Session recording, playback, and storage after the join

- Sessions recorded after the join are playable through SPP and are stored on the SPS appliance. An archive server can be set up through SPS.
- Sessions recorded prior to joining the Safeguard Sessions Appliances are not migrated to the SPS appliance. For that reason, it is recommended that the SPP sessions be migrated to an archive server prior to the join.

Functionality in SPS after the join

The following functionality handled in SPP's user interface is available in SPS after the join.

- Session certificate assignment is handled by SPS. The certificate is available for audit by the Auditor.
- After the join, you will set the following configurations in SPS. There is no migration of the SPP settings added via **Administrative Tools** | **Entitlements** | **Access Request Policies** | **Session Settings**. These include:
    - Session recording
    - SSH related command detection and controls (such as SFTP, SCP, and X11 forwarding)
    - RDP related command detection and controls (such as Windows title detection and allowing the clipboard)
- In SPS, you will:
    - Set the SSH banner text that is shown to session users when they initiate a privileged session notifying them the session will be recorded.
    - Identify the SSH host key presented to the user's SSH client when an SSH session is started.
    - Identify the status of the session module, such as session module health.
    - Edit the default policy.

The primary provider names must match for a SPS initiated connection with SPP. See KB article 311852.

Functionality in SPP after the join

- During the join, 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 join. These include: **General**, **Scope**, **Requester**, **Approver**, **Reviewer**, **Access Config**, **Time Restrictions**, and **Emergency** tabs.

- The Activity Center shows all old sessions and new sessions per the configuration. You can play back a session from SPP. However, the session index, which makes the privileged users' activity searchable, is only available from SPS.
- Entitlement reports have not changed.
- On the Dashboard, administrators can still view and manage access requests and accounts failing tasks as usual.
- After the join, **Administrative Tools** | **Settings** | **Sessions** functionality is no longer available and is handled via SPS. This includes session recording management, sessions module, SSH banner, and SSH host key.

Step 1: Prepare for the join

Move all session recording files from Safeguard for Privileged Passwords to an archive server.

1. The SPP embedded sessions module was remove in SPP 6.0 LTS so this step should have been completed earlier. If not, move the SPP embedded sessions recordings from local SPP to an archive server.
    - If the join has not been started, you can use the SPP user interface to archive existing SPP sessions:
        1. Set up the archive server. Navigate to For more information, see Archive servers on page 344.
        2. Assign the archive server to the SPP appliances. SPP moves the files and deletes the local file storage.
        3. Verify the recordings have been archived by comparing the session events in the Activity Center with the actual recording files on the archive server.
        4. Test the playback of a recording stored on the archive server. You will need to download it before you can play it. For more information, see Replaying a session on page 142.
    - If the join is complete, use the API to archive existing SPP sessions.
        a. Use the API PUT Core/v2/SessionArchiveConfigs/{id}. Call this API giving it the ID of the archive server (GET Core/v2/ArchiveServers) and the ID of the appliance (GET Core/SessionArchiveConfigs). Calling the above POST API will assign an archive server to archive session recordings. Within a few minutes, all remaining recordings will be moved to the archive server and removed from the local SPP storage.
        b. Test the playback of a recording stored on the archive server. You will need to download it before you can play it. For more information, see Replaying a session on page 142.
2. Ensure the join is performed when open access requests are not pending, if possible.

When the SPS session connection is joined, open access requests are automatically closed. When you double-click the event in the Activity Center, the event details **Action** is **Evicted**.

3. Back up your appliances and archive servers. For more information, see Backup and Retention settings on page 343.

Step 2: Join SPS and SPP

The join is initiated from Safeguard for Privileged Sessions. For details about the join steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide*.

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 an SPS 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 SPS 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 SPS nodes and roles, see the *One Identity Safeguard for Privileged Sessions Administration Guide*: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Step 3: Perform post join activities in SPP and SPS

Steps to perform in SPP

1. The Appliance Administrator assigns the managed networks for sessions management.

   Navigate to **Administrative Tools** | **Settings** | **Cluster** | **Managed Networks**. For more information, see Managed networks on page 369.

2. The Appliance Administrator can view, delete, or edit join connections, as needed.

   Go to **Administrative Tools** | **Settings** | **Cluster** | **Session Appliances**. For more information, see Session Appliances with SPS join on page 377.

   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 rejoin and reestablish the SPS Connection Policy via **Administrative Tools** | **Entitlements** | **Access Request Policies** | **Session Settings**. 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 **Administrative Tools** | **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 **Session Settings** 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 join does not affect the settings on the tabs including the **General**, **Scope**, **Requester**, **Approver**, **Reviewer**, **Access Config**, **Time Restrictions**, and **Emergency** tabs.

Steps to perform in SPS

Complete any set up in SPS 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 join

If you add another SPS cluster after the initial join, follow these standard operating procedures:

1. Add join connections. For more information, see Session Appliances with SPS join on page 377.
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 on page 276.
3. Assign the managed networks. For more information, see Managed networks on page 369.

Appendix D

Regular expressions

Regular expressions are used to parse large amounts of data to find matching patterns and validate a predefined pattern. For example, in Safeguard for Privileged Passwords, 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 Ticketing systems on page 417.

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.

Glossary

SPP glossary

A

access request
Rule-based password request and/or session request for an account. Access can be automatically approved or require one or more approvals. Email or toast notifications can be set.

access request broker
With the Application to Application service, a third-party application can create an access request on behalf of another user.

access request policy
Settings that restrict system access. Used to manage access (for example, to a password release request policy or session request policy). Defines the scope (assets, asset groups, accounts, or account groups), the access type (password, SSH, RDP, or telnet), and the rules for password check out (duration and number of approvals). Entitlements are sets of access request policies.

access request policy time restrictions
Enforce when a user can access the account passwords. If there are entitlement and policy time restrictions, the overlapping period is valid.

account
May be a directory account or service account associated with an asset. An account can only be associated with one asset. Accounts are added to policies for management (for example, to a password release request policy or session request policy). An account may be associated with an entitlement, account group, or both. Also see user.

account dependency
SPP maintains the passwords for dependent accounts on all the systems that use them (for example, one or more Windows servers use a directory account, such as an Active Directory account, to run services or tasks).

Account Discovery job
Job with rule-based settings to discover all accounts assigned to the assets in a selected partition, are made available globally, or only the accounts that match the

rules criteria. You can automatically manage the found accounts and automatically discover and configure dependent systems. Or, you can manually add the discovered accounts.

account group
A set of accounts that can be added to the scope of an access request policy, which in turn can be associated with an entitlement. See dynamic account group.

AD (Active Directory)
Microsoft AD consists of services running on a Windows Server to manage permissions and access to networked resources. AD stores data as objects.

AD FS (Active Directory Federated Services)
A software component developed by Microsoft that runs on a Windows Server operating systems to provide users with single sign-on access to systems and applications located across organizational boundaries.

appliance
The SPP appliance is hardware with pre-installed software to for easy installation. The appliance is hardened to ensure security at the hardware, operating system, and software levels.

Appliance Administrator
Responsible for configuring and maintaining the SPP appliance.

Application to Application (A2)
An SPP service where third-party applications can retrieve a credential from SPP to 1) perform automated functions or 2) allow a user to log in to SPP to retrieve a password or start a session.

Approval Anywhere
SPP feature where an approver can approve (or deny) access requests through their mobile device.

archive servers
External physical servers where you store backup files.

asset
A computer, server, network device, directory, or application managed by Safeguard for Privileged Passwords. You can log in to an asset with more than one account, but an account (user, group, or service) can only be associated with one asset. All assets must be governed by a partition profile. Assets may be subdivided into subsets for management. For example, a directory asset can manage a subset of the forest.

Asset Administrator
Manages all partitions, assets, and accounts.

Asset Discovery job
Job with rule-based settings to discover and add assets that are not in SPP. A job can be run against a directory or network (IP range).

asset group
A set of assets that can be added to the scope of an access request policy, which in turn is associated with an entitlement. See dynamic asset group.

asset tag rules
Can be set to dynamically add tags to assets and asset accounts so the assets and asset accounts can be identified and added to dynamic groups.

audit log management
Tasks defined and scheduled to purge audit logs from the SPP Appliance and archive older audit logs to a designated archive server.

audit log signing certificate
Used to sign the audit log files saved to an archive server. Proves that the audit logs were created by and came from a particular SPP cluster.

Auditor Administrator
Role with read-only access to all features to review all access request activity.

authentication
Authentication is the process of validating an identity provided to a system. For example, a system checks the user's login name and password. In SPP, a user's identity provider and authentication provider can be the same or different.

authentication provider
In SPP, any mechanism that a user enters credentials into to prove they are acting on behalf of a specific user or system, but does not necessarily contain any personal information of the user. An authentication provider can be the same as the identity provider (such as Active Directory). See identity provider.

Authorizer Administrator
Creates and maintains users, directory groups, directory users, password rules, and passwords. Unlocks and enables or disables local and directory user accounts. Typically unlocks administrator accounts.

auto-login
Automatic login that never exposes the account credentials to the user.

B

backup and retention settings
Used to manage SPP backups and archive servers. SPP encrypts and signs the data before the data is made available for downloading to an off-appliance storage.

Bootstrap Administrator
A built-in account to use to start up the appliance for the first time. The account is used to create other administrators. The Bootstrap Administrator default password should be changed. All actions are audited.

C

CA (certificate authority)

The authority that issues SSL certificates that are publicly trusted by web browsers. Anyone can issue SSL certificates but the certificates are not automatically trusted by web browsers.

certificate (SSL certificate)

A small file installed on a secure server that digitally binds a cryptographic key to a computer, device, individual, or organization. A certificate is used to establish trust for communication. Certificates contain information identifying the owner of the certificate, the public key, the expiration date of the certificate, the name of the CA that signed the certificate, and some other data.

certificate settings

Used to manage the certificates that are used to secure SPP. Some SPP certificates are default and need to be replaced and others are user-supplied certificates.

certificate store

A special key database file that Digital Certificate Manager (DCM) uses to store digital certificates. In SPP, the certificate store is owned by the cluster. SSL certificates in the store can be added to any appliance in the clustered environment.

change password

For user and service accounts, the rules and process to reset and synchronize the user or service account password with the SPP database. For directory accounts, SPP synchronizes the directory account password provided by an external identity provider, such as Active Directory. Also see check password and set password.

check password

For user and service accounts, the rules and process to verify the account password is in sync with the SPP database. If the password verification fails, you can change the password. Check passwords is associated with a partition. For directory accounts, the rules and process to verify the directory account passwords (such as Active Directory) and synchronize with SPP. Also see change password and set password.

CIDR (Classless Inter-Domain Routing)

Allows flexible allocation of Internet Protocol (IP) addresses. A CIDR network address under IPv4 looks like: 192.20.250.00/18. The network address is 192.20.250.00 and the 18 indicates that the first 18 bits are the network part of the address that leaves the last 14 bits for specific host addresses.

clone of VM

A copy of an existing virtual machine (the parent) that is a separate virtual machine which may share virtual disks with the parent virtual machine.

cloud platform account

SPP can manage cloud platform accounts such as Amazon Web Services (AWS).

cluster
A set of computers that work together where each replica (node) can perform the same task to enable high availability and load distribution.

consensus (quorum)
A cluster has consensus (quorum) when the majority of the members (primary or replica appliances) are online and able to communicate.

credential retrieval
With the SPP (Application to Application service), a third-party application can retrieve credentials from SPP outside the normal workflow.

CSR (certificate signing request)
A CSR is submitted to a certificate authority (CA) to obtain a digitally signed certificate.

CSS (cascading style sheet)
A .css file that describes how HTML elements display on screen, paper, or other media. See HTML5.

csv
A file format used with programs that store data in tables, such as Microsoft Excel. CSV stands for Comma-Separated Values.

custom platform
Platform added to SPP via uploading a custom platform script. The script may be selected when adding or updating an asset. Custom platforms are global across all partitions.

D

DCM (Digital Certificate Manager)
Used to manage digital certificates on a network and use Secure Sockets Layer (SSL) to enable secure communications for applications.

default gateway
The access point or IP router that sends information to a computer in another network when no other route specification matches the destination IP address of a packet.

default SSL certificate
SPP provides a default self-signed SSL certificate for HTTPS assigned to the appliance. This certificate is not a trusted certificate and should be replaced.

delegated owner
One or more users that the Asset Administrator selected to manage the assets and accounts in a partition.

deny
An active access request can be either denied or approved. An approved active access request can be revoked.

directory
A structure to catalog files and, possibly, other directories. In SPP, the structure and objects from a directory service, such as Active Directory or OpenLDAP, can be imported and synchronized.

directory account
An account from an external identity store, such as Microsoft Active Directory, used to authenticate to a managed system (asset).

DNS (Domain Name System)
System to translate human readable information (such as a domain name, web site, or other internet-based resource) to the addressing protocols (IP address).

DNS server (domain name server)
Contains a database of public IP addresses and their associated hostnames and translates the common names to IP addresses.

domain name
The name of a network (for example, oneidentity.com).

dynamic account group
Account group made up of systematically identified accounts that meet asset account rules, directory account rules, or both. The rules engine runs when you add or change an asset account or an asset account rule.

dynamic asset group
Asset group made up of systematically identified assets that meet identified rules.

dynamic disk
Fault-tolerant volumes that may span multiple disks; flexible volume management with database tracking and replica storage of the dynamic disk database.

E

entitlement
A set of access request policies that restrict system access (including rules and schedules), typically by job role. Entitlements are used to authorize users or user groups for accounts in the scope of the access request policies. Entitlements can be associated with one or more profiles.

entitlement time restrictions
Controls identifying when an entitlement is in effect (user's time zone). If there are both entitlement and policy time restrictions, the overlapping period is valid.

explicit association (explicit assignment)
You can explicitly add an asset to a profile. This overrides the implicit inheritance from the partition so the asset's profile is no longer determined by the partition. You can explicitly assign an account to a profile the account's profile is no longer determined the asset.

F

factory reset
Operation to recover from major problems or clear appliance data and configuration settings. All data and audit history are removed.

federation metadata
The data format for communicating configuration information between an identity (claims) provider and a relying party. The data format is defined in Security Assertion Markup Language (SAML) 2.0, and it is extended in WS-Federation.

federation provider
Service provider that mediates between two or more trust domains so users can access applications and services using the same digital identity.

FIDO2 (Fast ID Online)
A set of security specifications for strong authentication. FIDO2 supports multifactored authentication, public key cryptography, biometric authentication, and other personally identifying information (PII).

forest
Network logical division that may contain one or more trees and in turn domains made up of objects (computers, users, devices) sharing the same database. The first domain in the forest is called the forest root domain.

FQDN (fully qualified domain name)
A domain name that specifies its exact location in the tree hierarchy of the Domain Name System (DNS). For example, given a device with a local hostname myhost and a parent domain name example.com, the fully qualified domain name is myhost.example.com.

G

gateway
A device that connects two or more parts of the network. For example, the device may connect your local intranet and the external network (the internet). Gateways act as entrances to other networks.

GMT (Greenwich Meridian Time)
GMT is never out of sync with UTC (Coordinated Universal Time) by more than nine tenths of a second so UTC and GMT are virtually equivalent in common usage.

H

HA (high availability)
A system that is resilient and likely to operate continuously without failure for a long period of time.

Help Desk Administrator
Sets passwords for non-administrative user accounts and unlocks user accounts. The Authorizer Administrator typically unlocks administrator accounts.

host
A computer connected to the network. A host may offer resources, services, and applications to users or nodes on the network. May have virtualization software (such as ESX or ESXi) to run virtual machines (VMs).

hostname
A label assigned a device connected to a network and that is used to identify the device.

HTML5
Hypertext Markup Language version 5 is the code that describes web pages and includes HTML for structure, Cascading Style Sheets (CSS) for presentation, and JavaScript (processing).

I

identification
Identification happens when a user claims to be a specific system user. For example, a user's login name and password are used to establish identity. In SPP, a user's identity provider and authentication provider can be the same or different.

identity provider
In SPP, the source from which the user's personal information comes from and is synchronized with. See authentication provider.

implicit association (implicit assignment)
When an asset is added, it is added to the default partition and default profile (implicit association/assignment). Accounts inherit the parent asset's profile. This can be overridden by explicitly assigning an asset to a profile; the asset's associated accounts are also assigned to the new profile.

import
Accounts, assets, or users in a Comma Separated Values (.csv) file can be added to SPP's database. Objects must pass validity tests. Default values may be added during the import.

IP address (Internet Protocol address)
Unique internet number assigned to each device communicating across the internet. The IP address provides location and identification. See DNS.

IPv6 (Internet Protocol version 6)
The most recent version of the Internet Protocol (IP). See IP address.

J

JavaScript
A computer programming language commonly used for processing on the web. See HTML5.

json
A language-independent data format. Code for parsing and generating JSON data is readily available in many programming languages. JSON stands for "JavaScript Object Notation".

K

key pair
A private key and its related public key. The private key is known only to the owner, while the public key can be freely distributed. Information encrypted with the private key can only be decrypted using the public key.

KMS (Key Management Service)
Used to activate systems in the organization's network so that individual computers do not have to connect to Microsoft for product activation.

KMS Server (Microsoft Key Management Server)
A Microsoft Volume Activation 2.0 solution service used to activate volume licensed Microsoft products.

L

LDAP (Lightweight Directory Access Protocol)
An application protocol for querying and modifying data using directory services running over TCP/IP.

lights out management (via BMC/baseboard management controller)
Feature to manage the SPP power state and serial using BMC. This feature is used to power on an appliance remotely or to interact with the Recovery Kiosk.

M

MAC (Media Access Control) address
An identifier assigned to a network adapter or any device with built-in networking capability (such as a printer). A MAC address is burned into the device at the factory (versus an IP address that is assigned later). Also called a hardware address or physical address.

Mac keychain
The Apple password management system in Macintosh OS X.

managed networks
Named lists of network segments serviced by specific SPP Appliances in a clustered environment. Used to distribute the task load by scheduling tasks (for example, password change or asset discovery).

MSI
MSI is an installer package file format used to launch Windows-based software installations.

N

netmask
For IPV4, a 32-bit mask used to divide an IP address into subnets and specify the network's available hosts.

network interface and proxy server
Network interface X0 is the primary interface. Proxy server X0 is for relaying web traffic if the devices don't connect to the web.

NS lookup (named service lookup)
Network utility program to obtain information about internet servers. It finds name server information for domains by querying the domain name server (DNS).

NTP (Network Time Protocol)
Protocol to synchronize computer clock times in a network.

O

Offline Workflow Mode
Appliance state when the appliance no longer has consensus (quorum) and has been enabled to process access requests using cached policy data. The appliance operates in isolation from the remainder of the cluster.

Operations Administrator
Monitors the status of the appliance and can reboot the appliance. This role can be a script or external monitoring system.

OU (Organizational Unit)
A subdivision within an Active Directory into which you can place users, groups, computers, and or any other organizational units (for example, functional or business hierarchy.

OVA (Open Virtualization Appliance)
An OVA file contains a compressed version of a virtual machine (VM) to be installed. When you open an OVA file, the VM is extracted and imported into the virtualization software installed on your computer.

P

partition

A group of assets (and the assets' associated accounts) governed by a partition profile and used for 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 but can be reassigned.

partition profile

The schedules and rules that are required to govern a partition's assets and the assets' accounts. You can set a default partition profile to assign to assets and assets' accounts. You can manually assign a partition profile to an asset or account.

password rules

The requirements for user password authentication, such as uppercase and lowercase letters, numerics, and special characters. Password rules set in SPP apply to local users not users from external providers such as Active Directory.

password sync groups

Used to control password validation and reset across all associated accounts.

ping

A command that sends a message from a host to another host over a network to test connectivity and packet loss.

port

A number from 1 to 65,535 for the destination application of the transmitted data. For example, SSH commonly uses port 22 and web servers (HTTP) commonly use port 443.

primary appliance

One appliance in a cluster where vital data stored on the primary is also stored on replica appliances.

primary authentication

The first authenticating factor for a remote user when two-factor authentication (2FA) is enabled.

priority precedence

In authorizing password check-out, SPP first considers the entitlement priority then considers the priorities of access request policies in the entitlement.

profile

See partition profile and directory profile.

PuTTY

A free and versatile terminal tool for remote access to another computer.

R

RBAC (role-based access control)
The role-based access control model restricts system access to authorized users based on roles. SPP supports this model.

RDP (Remote Desktop Protocol)
A Microsoft proprietary protocol that provides graphical user interface to connect to another computer over a network connection.

regular expression
A string that describes or matches a set of strings.

relying party
A service or application, like Safeguard, that receives and accepts a SAML assertion issued by a SAML authority.

REST
Architecture that allows other applications and systems to integrate with diverse systems and applications. SPP's API is based on a REST architecture.

revoke
An approved active access request can be revoked.(An active access request can be either denied or approved.)

root SSL certificate (trusted certificate)
A certificate issued by a trusted certificate authority (CA) at the top of the trust chain and used to issue intermediate SSL certificates to ensure the security of the system.

S

SAML (Security Assertion Markup Language)
An open standard for sharing security information about identity, authentication and authorization across systems. SAML is implemented with the XML standard for sharing data. SAML provides a framework for implementing single sign-on and other federated identity systems.

scope
An access request policies assets, asset groups, accounts, or account groups assignments.

Secure Shell (SSH)
A security protocol for logging in to a remote server.

security key
A small physical device that is inserted into a USB drive. Typically, you will enter your password then insert the security key as a required second form of authentication. You can use one security key with more than one account. You can

have multiple security keys registered on an account. Activating the registration of a security key varies with the key (for example, press a button or tap). Security keys must be U2F or WebAuthn capable.

Security Policy Administrator
Creates account groups, asset groups, and user groups. Creates entitlements and adds users or user groups to entitlements. Configures access request policies.

service account
Used by an application or service to interact with the operating system or configuration.

service account domain name
The name of the domain where the service account resides. SPP uses DNS-SRV to resolve domain names to actual domain controllers.

Service Discovery job
Scans Windows assets and automatically discovers Windows services and tasks. If the directory accounts are managed by SPP, the service or task is automatically associated with the managed account. Administrators can identify unmanaged accounts to potentially manage.

sessions
SPP issues privileged access to users for specific periods, called sessions.

set password
Rules and process to manually set or randomly generate the user or service account passwords in the SPP database. The process does not change the account password on the asset. For directory accounts, SPP synchronizes the directory account password provided by an external identity provider, such as Active Directory. Also see check password and change password.

SID (Security IDentifier)
An alphanumeric name used to identify user, group, and computer accounts in Windows. SIDs are created an account is first created in Windows and no two SIDs on a computer are ever the same.

SMTP server (Simple Mail Transfer Protocol server)
Protocol server that handles email delivery process (for example, smtp.gmail.com).

snapshot of VM
The state of a computer system at a point in time. Snapshots are not enough to restore a virtual machine and do not replace backukps.

SNMP (Simple Network Management Protocol)
An industry standard protocol for network management. SNMP alerts are sent to a central SNMP server.

SPA
One Identity Safeguard for Privileged Analytics solution to monitor behavior and identify threats.

split brain
A split brain situation occurs when for some reason (for example, the loss of connection between the nodes) both nodes of a cluster become active as the primary. New data (for example, audit trails) may be created on both nodes without being replicated to the other node. Thus, it is likely in this situation that two diverging sets of data are created that cannot be easily merged.

SPP
One Identity Safeguard for Privileged Passwords solution to secure privileged credentials.

SPS
One Identity Safeguard for Privileged Sessions solution to control, monitor, and record privileged sessions.

SSH (Secure Shell) key
An access credential in the SSH protocol. The function is similar to a user name and passwords, but SSH keys are primarily used for automated processes and for implementing single sign-on to an SSH server by system administrators and power users.

SSH authorized key
The public key from an SSH identity key pair.

SSH banner
Contains security warning information or general information.

SSH host key
Used for authentication. Host keys are pairs. Public host keys are stored on or distributed to SSH clients. Private keys are stored on SSH servers.

SSH identity key
An SSH key pair used for SSH 'publickey' authentication. The private key is required to prove identity and log in wherever the key is authorized.

SSH key
An access credential in the SSH protocol. Functionally similar to a user name and password, but primarily used for automated processes and single sign-on by system administrators and power users.

SSH settings
Parameters of the connection on the protocol level, including timeout value and greeting message of the connection, as well as the encryption algorithms used.

SSL
Secure Sockets Layer (SSL) is a cryptographic protocol that provides secure communications on the internet.

SSL certificate store
Contains uploaded or enrolled SSL certificates owned by a cluster. Any SSL certificate in the store can be assigned to any appliance in the clustered environment.

SSO (single sign-on)
User logs in with a single ID and password per session to gain access to multiple services within a single organization.

STS (Security Token Service)
A third-party servce responsible for issuing, validating, renewing, and cancelling security tokens. The tokens are used to identify the holder of the token to services that adhere to the WS-Trust standard.

support bundle
System and configuration information sent to One Identity Support to analyze and diagnose issues.

syslog
Protocol to produce and send log and event information from Unix/Linux and Windows systems and devices over UDP port 514 to a centralized syslog server.

T

tags
Can be assigned manually (static) or dynamically set through tagging rules (identified by a lightning bolt icon). Tags are helpful in searches. Dynamic tags are updated when the rules engine runs when you add or change an asset account or an asset account rule.

TCP/IP (Transmission Control Protocol/Internet Protocol)
A set of networking protocols that allows two or more computers to communicate.

telnet
A terminal emulation protocol that enables a user to connect to a remote host or device using a telnet client.

thumbprint
A unique hash value that identifies the certificate.

ticketing feature
SPP can be integrated with a company's external ticket system, such as ServiceNow or Remedy.

TLS (Transport Layer Security)
TLS and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the internet. The application can encrypt the communication between the clients and the server using TLS to prevent unauthorized access to sensitive log messages.

toast notifications
A small, auto-expiring alert that displays when the desktop client application is not the active foreground application.

traceroute
A command that shows all routing steps (the path of a message) between two hosts.

traffic shaping (packet shaping)
Manipulates and prioritizes network traffic to reduce the impact of heavy use cases from effecting other use cases.

two-factor authentication (2FA)
A user is required to provide two different authentication factors to verify themself. Provides a higher level of security than one factor and protects the user's credentials and the resources accessed.

U

UNC (Universal Naming Convention) path
Used to access network resources and contains two or more of the following components: \\<servername>. <share>.<filename>

user
A person who can log in to SPP. A user can be local or 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 may or may not have administrator permissions.

User Administrator
Creates (or imports) users. Sets passwords, unlocks accounts, and enables or disables non-administrator user accounts. Adds directory groups to directories, including directory users. Grants Help Desk Administrator permissions. The Authorizer Administrator typically unlocks administrator accounts.

user group
A set of local users or directory users that can be added to an entitlement to use the entitlement’s access request policies restricting system access.

UTC (Coordinated Universal Time)
UTC is never out of sync with GMT (Greenwich Meridian Time) by more than nine-tenths of a second, so UTC and GMT are virtually equivalent in common usage.

V

virtual machine (VM)
A software computer that runs an operating system and applications and acts as an isolated computing environment. One host computer may have multiple virtual machines.

W

web console

A web-based application that allows you to execute shell commands on a server directly from a browser (web-based SSH).

WMI (Windows Management Instrumentation)

The infrastructure for accessing management data in an enterprise environment. You can write WMI scripts or applications to automate administrative tasks on remote computers. WMI also supplies management data to other parts of the operating system and products.

workflow engine

Directs workflow and may include time restrictions, reviewers, approvers, emergency access, and policy expiration. May integrate with a ticketing system and have reason codes.

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.

Index

3

3270
- session access request setup 569

5

5250
- session access request setup 569

A

access API 49
Access Config tab 284
access historical information 561
Access Key, about 211
access request broker 383
Access Request Policies tab
- account 150
- account group 169
- asset 188
- asset group 225
- entitlement 269

access request policy
- access settings 284
- add account 177
- approver settings 280
- assign accounts and assets 278
- emergency access 286
- requester settings 279
- reviewer settings 282
- session access settings 285
- time restrictions 286

Access Request Policy dialog
- Access Config tab 284
- Approver tab 280
- Emergency tab 286
- General tab 277
- Requester tab 279
- Reviewer tab 282
- Scope tab 278
- Session Settings tab 285
- Time Restrictions tab 286

Access Request settings 309
- Enable or Disable Services 309
- Reasons 312

access request states 575
access request workflow 117
access requests
- enable for service account 202
- enable or disable services 309
- view details 93

Access Requests dashboard
- about 92
- view details 93

account
- about 147
- Access Request Policies tab 150
- Account Groups tab 151
- add 156, 176
- add cloud platform account 157
- add dependent account to a Windows server 217
- add to access request policy 151-152

add to account group 151, 153, 159, 168, 176, 189
add to profile 304
associate with asset 186, 215
associated asset 149
change password 160
Check and Change Log tab 153
check and set password 165
General tab 148
History tab 154
manually add tag 159
modify 160
remove 161
select account group 159
unlock 466
account dependencies
about 216
add to Windows servers 217
Account Dependencies tab
asset 188
account discovery
add setting 235, 249, 252, 333
delete job 259
delete setting 235, 249, 333
details 249
discover accounts 249
discover service accounts 249
edit job 258
how to setup 251
modify setting 235, 249
run setting 235
view setting 235
account discovery job
about 248
account discovery rule
add 254
account group
about 167
Access Request Policies tab 169
Accounts tab 168
add 160, 172
add a dymanic group 173
add account 159, 176
add to policy 177
General tab 168
History tab 170
History tab membership operation 155, 171, 272, 299, 450, 471
modify 177
remove 178
Account Groups tab
account 151
account password
change 165
check 165
set 165
account password rules
about 421
add 421, 423
add to profile 303
copy 422
delete 422
modify 422
Accounts tab
account group 168
asset 186
ACF - Mainframe systems
prepare for Safeguard 520
activate read-only appliance 492

Activity Center
about 94
apply search criteria 95
audit request workflow 102
delete saved search 101
delete scheduled report 101
edit saved search 101
edit scheduled report 101
generate report 97
query builder 95
save search criteria 97
schedule report 99
activity events
filtering report results 103
view details 102
add
account 147, 156
account dependency to Windows severs 217
account discovery rule 254
account discovery setting 235, 249, 252
account group 160, 167
account groups 172
account password rules 423
account to access request policy 177
account to asset 215
accounts to account groups 176
application registration 386
asset 180, 193
asset group 223, 228
asset or account to partition profile 305
asset to asset group 218
asset to partition 301
audit log signing certificate 358
cloud platform account 157
custom platform 333
directory group 474
dynamic account group 173
dynamic asset group 228
dynamic asset or asset account tag 337
entitlement 266, 273
external federation provider trust 562
external federation user account 564
license 321
managed network 373
partition 292, 300
password reset schedule 426
password sync group 433
password validation schedule accounts 430
trusted certificate 364
user 444, 451, 564
user group 467, 473
user group to entitlement 288
user group to role 477
user to entitlement 288
user to role 459
user to user group 476
admin password reset 58
Administrative Tools 107
administrator
permissions 507
administrator permissions
Appliance Administrator 507
Asset Administrator 509
Auditor Administrator 511
Authorizer Administrator 512
Help Desk Administrator 513

Operations Administrator 514
Security Policy Administrator 516
User Administrator 517
Administrator widget
about 547
Amazon Web Services platforms
prepare for Safeguard 521
API
access 49
customize response 52
EventSubscribers 397
query filtering 52
API key
regenerate for Application to Application service 388
appliance
activate 492
add license 321
appliance name, set 318
Appliance settings 313
assign SSL certificate 363
backup and restore cluster 495
diagnose cluster 492
diagnostics package 59, 315
factory reset 320, 498
information 58
LCD controls 545
LDD status messages 544
Lights Out Management (BMC) 322
modify network suffixes 327
monitor cluster health 367
networking settings 326
patch cluster members 493
remove from cluster 483
reset cluster 497
restart 319, 544, 552
shut down 318, 552
specifications 31
states 502
time 330
unjoin from cluster 483
update license 321
view information about 315
virtual appliance setup 42
Appliance Administrator permissions 507
appliance configuration
about 381
NTP server 331
appliance diagnostic package 59, 315
Appliance Diagnostics
settings 59, 315
Appliance Information
restart appliance 319
settings 315
shut down appliance 318
Appliance settings 313
application registration
add 386
delete 388
Application to Application
about 383
add registration 386
delete registration 388
regenerate API key 388
setting up 385
settings 382
Application to Application service
check status 383
disable service 319
enable 383

enable service 319
make request to 388
apply search criteria to a activity audit log 95
Approval Anywhere
configure 393
approve password release request 126, 137
desktop client 126
approve session access request 137
Approver tab 280
archive backup file 354
archive servers 344
configure 345
delete configuration 345
modify configuration 345
asset
about 179
Access Request Policies tab 188
Account Dependencies tab 188
Accounts tab 186
add 193
add dynamic tag 337
add to asset group 224, 231
add to partition 306
add to partition profile 303
add to partitions 301
associate account with 186, 215, 219
authentication types 200
copy tag to another partition 342
delete tag 341
Discovered Services tab 190
General tab 182
hide asset marked "ignore" 148, 180
History tab 191
import 180
link to profile 213-214
modify 218
modify connection timeout 218
modify tag 341
product (operating system)
not modifiable 196
remove 219
show hidden 148, 180
view tag assignments 342
asset account
add dynamic tag 337
copy tag to another partition 342
delete tag 341
modify tag 341
view tag assignments 342
Asset Administrator permissions 509
asset authentication type
access key 203, 211
none 207, 211
password 208
Asset dialog
Connection tab 200
General tab 194
Management tab 195
asset discovery
about 234
add new job 236
General tab 237
Information tab 238
Rules tab 239
Asset Profile 245
Condition 240
Connection 242
Schedule tab 245
Summary tab 246

delete job 247
directory scan 238
edit job 246
network scan 238
asset group
about 223
Access Request Policies tab 225
add 228
add account to 231
add asset to 218
add dynamic group 228
Assets tab 224
General tab 224
History tab 226
History tab membership operation 192, 226
modify 232
remove 232
view 223
Asset Management settings 332
Assets tab
asset group 224
assign accounts and assets to access request policy 278
assign user to partition 459
Audit Log Management settings 346
Audit Log Signing certificate 356
audit log signing certificates
add 358
create CSR 359
audit request workflow 102
Auditor Administrator permissions 511
Authentication tab 453
Authorizer Administrator permissions 512
AWS 63
backup and recovery 57, 66
change setup 63
deployment steps 63
IP settings 63
security 63
Azure 64
backup and recovery 57, 66
change setup 64
deployment steps 64
IP settings 64
security 64

B

backup
about 343
archive 349
archive backup file 354
clustered appliance 495
configure archive server 345
create 349-350
delete 349
download 349, 352
information 348
restore 349, 353
run now 349
schedule 350
upload 349, 352
Backup and Retention settings 343
Archive Servers 344
Audit Log Management 346
Safeguard Backup and Restore 348
Safeguard Backup Retention 354
backup retention setting
enable 354

Best Practice
Add service accounts to profiles set to never change passwords 202
Add User Groups as approvers or reviewers rather than individuals 281, 283
After changing a user's administrative permissions, close the user's connections to the appliance 461
Disable directory users instead of deleting 462
Keep a minimum number of backups on the appliance 348
Perform backups more frequently than the Maximum Password Age setting 350
Setup an NTP server to eliminate system time issues. 571
bootstrap admin password
reset 552

C

Cannot 543
certificate settings 355
Certificate Signing Request 359
create for audit logs 359
SSL certificate 362
certificate support for telnet 521, 525, 528, 534
certificates
about 355
Audit Log Signing 356
CSRs 359
how to prevent messages when making RDP connections 567
install audiot log signing certificates 358
RDP Connection Signing Certificate 356
Session Recording Signing Certificate 356
Timestamping Authority Certificate 356
challenge response process 58
change password 160
change password management
disable 311
enable 311
change password setting
about 425
add to profile 302
copy 426
delete 426
modify 426
Check and Change Log tab
account 153
check asset connectivity
about 212
check password management
disable 310
enable 310
check password setting
about 429
add to profile 302
copy 430
delete 430
modify 430
Cisco devices
prepare for Safeguard 521
cloud
AWS 61, 63
Azure 61, 64
backup and recovery 57, 66

change setup 63-64
using 61
using AWS 63
using Azure 64
cloud platform account
add to Safeguard 157
cluster
about 479
appliance details 366-367
backup and restore 495
configurations 479
consensus 480
diagnose 492
failover to replica 491
health check 480
monitor health 366-367
patch 493
primary appliance 479
primary appliance failure 481
promote replica to primary 491
remove quarantined appliance 576
remove replica appliance 483
replica appliance 479
reset 481, 497
settings 365
troubleshooting tips 501
unjoin and activate 481
unjoin replica appliance 483
unlock 501
Cluster Management settings 366
cluster member
about cluster patching 494
Activate 485
Check Health 485
Diagnose 485
Failover 485
patch 493
Unjoin 485
Cluster monitoring page 365
cluster patching
failure scenarios 494
service guarantees 494
Cluster settings
Cluster Management 366
Managed Networks 369
cluster view pane 366
Cluster view pane 367
configure alerts 118
configure assets for Safeguard 519
Connection tab 200
contact information
change personal information 86
converting timestamps 106
copy
account password rule 422
asset or asset account tag to another partition 342
change password setting 426
check password setting 430
SNMP subscription 411
syslog server configuration 416
create relying party trust in IdP-STS 563
Creating
custom platform script 334
credential retrieval 383
custom platform
about 333
download script 334
view 333

custom platform script
create 334

D

delete
account 147
account discovery setting 235, 249
account group 167
account password rule 422
application registration 388
archive server configuation 345
asset 180
asset group 223, 232
asset or asset account tag 341
change password setting 426
check password setting 430
custom platform 333
entitlement 267, 290
external federation service provider configuration 399
managed network 374
partition 292
password sync group 433
saved search 101
scheduled activity audit log report 101
sessions management 380
SNMP subscription 410
Syslog server configuration 416
ticketing system 419
user 444
user group 467
dependent accounts
about 216
dependent system updates 217
desktop client
application settings 84
install 80
start 82
system requirements 35
uninstall 83
diagnostic tests
about 323
clustered appliance 492
nslookup 324
ping 323
show routes 326
Telnet 325
trace route 325
directories that can be searched 37
directory
add directory group 474
directory scan for assets 238
disable
change password management 311
check password management 310
password requests 310
session module password access enabled 312
session requests 310
toast notifications 118
disaster recovery
about 479
diagnose cluster members 485
maintain cluster members 485
troubleshooting tips 501
discover
accounts 249
service accounts 249
discovered services 190, 262

Discovered Services tab
partition 190
discovery
about 233
account 248, 258-259
account and service 251
asset 234, 236, 246-247
run now 190
asset discovery job workflow 236
Domain Name System (DNS)
set 566
download
custom platform 334
download Safeguard federation metadata 399
dymanic account group
add 173
Dynamic Account Group dialog
Asset Account Rules tab 174
General tab 173
Summary tab 176
dynamic asset group
add 228
Dynamic Asset Group dialog
Asset Rules tab 229
General tab 229
Summary tab 231
dynamic tag
add to assets or asset accounts 337

E

edit saved search 101
edit scheduled activity audit log report 101
email
administrative permissions determine what emails are sent 119
configure notifications 396
configure Safeguard to receive notifications 118
configure SMTP server 395
default events sent 119
modify templates 397
template macros 398
emergency access
about 270, 287
Emergency tab 286
enable
change password management 311
check password management 310
password requests 310
session module password access enabled 312
session requests 310
toast notifications 85, 118
Enable or Disable Services settings 309, 319
enroll cluster member 482
entitlement
about 266
Access Request Policies tab 269
add 273
add policy 290
add user 268, 288, 290
add user group 288, 470, 477
change priority 275
delete 290
expired 270
General tab 267

History tab 271
invalid 266, 270
membership 287, 459
modify 290
modify time restrictions 290
Policies tab 269
priority 274
time restrictions 276
Users tab 268
Entitlement dialog
General tab 273
Time Restrictions tab 275
entitlement report
filtering report results 103
Entitlements tab
user 447
user group 469
export
action bar option 98, 104
External federation
add external federation provider trust 562
add external federation user account 564
configure 561
create relying party trust in IdP-STS 563
external federation service provider
delete configuration 380, 399
modify configuration 380, 399
External Integration settings 381
Application to Application 382
Approval Anywhere 393
Email 395
External Federation 561
SNMP 411
Starling 412
Syslog 415-416
Ticketing 418

F

F5 Big-IP devices
prepare for Safeguard 523
factory reset 320, 498, 553
FAQ
How do access the API 49
How do I audit transaction activity 560
How do I configure external federation authentication 561
How do I customize the response using API query parameters 52
How do I manage account passwords manually 565
How do I prevent Safeguard prompt when making RDP connections 567
How do I require users to log in using secondary authentication 457
How do I require users to log in using two-factor authentication 455
How do I set the appliance system time 571
How do I set up telnet, 3270, and 5250 session access requests 569
How do Safeguard database servers use SSL 571
What are the access request states 575
What do I do when an appliance goes into quarantine 575
When does rules engine run for dynamic grouping and tagging 577

Why did the password change during an open request 578
favorites
create 88
remove 89
set color 89
federation metadata 561
download 399
download Safeguard federation metadata 562
manually input values 563
FIDO key 79, 86, 409
filtering report results 103
follow mode, session play back 143
Forntinet FortiOS devices
prepare for Safeguard 523

G

General tab
account 148
account group 168
asset 182
asset group 224
entitlement 267
partition 294
user 444
user groups 468
generate
activity audit log report 97
quarantine bundle 576
support bundle 554
global access request settings 309
glossary 599

H

Help Desk Administrator permissions 513
hide ignored assets 148, 180
History tab
account 154
account group 170
asset 191
asset group 226
entitlement 271
partition 298
user group 471
Home page
about 72, 90
navigation pane 89
HP iLO Management Processors
prepare for Safeguard 524
HP iLO servers
prepare for Safeguard 524
Hyper-V
backup and recovery 57, 66

I

IBM i (AS/400) systems
prepare for Safeguard 525
IdP-STS 561
create relying party trust 563
iDRAC devices
prepare for Safeguard 522
import
about 161, 219, 462
accounts 148
assets 180

create import file 164
CSV Template Assistant 164
file format 164
how to import objects 161, 219, 462
users 444
install
audit log signing certificate 358
desktop client 80
patch 332
SSL certificate 362
update file 332
integrate with Safeguard
external ticket system 418

J

join to Starling 412
JunOS servers
prepare for Safeguard 525

L

launch
RDP session 139
Safeguard Desktop Player 142
SSH client 138
LCD
controls 545
status messages 544
license
add 321
settings 321
update 321
licensing 45
Lights Out Management (BMC)
settings 322
Linked Accounts tab
users 448
live session
follow 143
terminate 143
Location tab 455
login control
configure 436
Login Notification setting 420

M

manage accounts passwords manually 565
managed network
add 373
delete 374
modify configuration settings 372
resolve IP address 374
Managed Networks
settings 369
Management tab 195
member
add to entitlement 287, 459
add to user group 446, 459, 476
Message of the Day setting 420
Messaging settings 420
MIBSNMP
configure subscriptions 411
Microsoft SQL Servers
prepare for Safeguard 531
SSL support 572
minimum required permissions for Windows assets 536
modify
account discovery setting 235, 249

account group membership 177
account information 160
account password rule 422
archive server configuration 345
asset group information 232
asset or asset account tag 341
change password setting 426
check password setting 430
email template 397
external federation service provider configuration 399
managed network 372
network suffixes 327
password sync group 433
sessions management 380
SNMP subscription 410
syslog server configuration 416
ticketing system 419
user password rules 439
MongoDB
prepare for Safeguard 526
MySQL servers
prepare for Safeguard 526
SSL support 573

N

network diagnostic tools 313
Network Interface X0 properties 326
network scan for assets 238
Network Time Protocol (NTP)
enable 331, 566
networking settings 326
new features and resolved issues 597
nslookup 324

O

object ID 108
ODBC Transport 572
Offline Workflow mode 480, 489
enable 490
resume operations 490
Operations Administrator permissions 514
Oracle databases
prepare for Safeguard 527
Other (or Other Linux) operating system
about 195

P

Palo Alto Networks
prepare for Safeguard 527
partition
about 21, 292
add 300
add asset 301
add assets 306
assign asset 213
change description 306
default profile 305
delegate management of 301, 306, 447
delete assets from 213
General tab 294
History tab 298
modify 306
Profile tab 297
reassign asset 302
reassign asset accounts 302
remove 307

Scope tab 295-296
set default 304, 306
partition profiles
add assets or accounts 305
Partitions
about 292
Partitions tab
user 446
password
change 86
change password manually 427
check and set 165
partition profile 194
policy, add to role 276
policy, modify 289
request, how to prevent 156, 215, 257
reset 465
viewing Password Archive 166
Password Archive
viewing 166
password check and change did not run 548
password Check and Change Log
view 154
password management services 309
password release
check-in 124-125
checkout 123, 125
password release request 121
cancel pending request 124-125
desktop client approval 126
desktop client check-in 124
desktop client checkout 124
disable 310
enable 310
remove request 124-125
resubmit request 124-125, 134, 136
review 127
web client approval 126, 137
web client check-in 123
web client checkout 123
workflow 120
password sync group
add 433
add to partition profile 304
change sync group password 433
delete 433
modify 433-434
priority 432, 434
password validation schedule
add 430
patch cluster members 493
permissions
about 507
Appliance Administrator 507
Asset Administrator 509
Auditor Administrator 511
Authorizer Administrator 512
delegated partition owner 459
Help Desk Administrator 513
Operations Administrator 514
Security Policy Administrator 516
User Administrator 517
Permissions tab 456
photo
change 86
ping 323
platforms that can be managed 37
play back recorded session 142

Policies tab
account 150
account group 169
asset 188
entitlement 269
policy
about 276
add accounts to scope 169, 225
add to role 269, 276
change priority 275
copy 289
edit 289
expired 266, 270
invalid 270
priority 278
reason codes 312
remove 288
time restrictions 276
view details 289
ports 580, 587, 592
PostgreSQL
prepare for Safeguard 527
power options 58
PowerShell 53
prepare asset for management 519
ACF - Mainframe systems 520
Amazon Web Services platforms 521
Cisco devices 521
Dell iDRAC devices 522
ESXi Hosts 522
F5 Big-IP devices 523
Fortient FortiOS devices 523
HP iLO Management Processors 524
HP iLO servers 524
IBM i (AS/400) systems 525
JunOS - Juniper Networks servers 525
MongoDB 526
MySQL servers 526
Oracle databases 527
PAN-OS Networks 527
PostgreSQL 527
RACF - Mainframe systems 528
SAP HANA 529
SAP Netweaver Application Servers 529
SonicOS devices 531
SonicWALL SMA or CMS appliances 531
SQL Server 531
Sybase (Adaptive Server Enterprise) servers 530
Topic Secret - Mainframe systems 533
Unix-based systems 534
Windows systems 535, 538
prevent Safeguard prompts when making RDP connections 567
priority
about 274
change entitlement priority 275
change policy priority 275
entitlement 274
policy 278
Privilege Elevation Command 204-205, 209
product licensing 45
profile
about 21-22, 293
add asset or account to partition profile 305
add to partition 297

assign to asset 214
explicit association 293
implicit association 293
reset default profile 293
Profile settings 421
Account Password Rules 421
Change Password 425
Check Password 429
profile, partition
about 297
add 302
add accounts 304
add assets 303
add password sync group 304
modify 303, 306
set as default 305
Profiles tab
partition 297
Proxy Server X0 properties 327

Q

quarantine bundle 576
quarantined appliance 575

R

RACF - Mainframe systems
prepare for Safeguard 528
RDP connection prompts 567
RDP Connection Signing certificate 356
RDP session
launch 139
read-only appliance
activate 492
reason codes 312
recover a quarantined appliance 575
recovery kiosk 549
appliance information 551
factory reset 553
generate quarantine bundle 576
generate support bundle 554
reboot appliance 552
reset bootstrap admin password 552
shutdown appliance 552
regnerate API key 388
remove
asset group 232
quarantined appliance from a cluster 576
trusted certificate 364
replay recorded session 142
replica
failover to replica 491
promote to primary 491
remove 483
unjoin 483
Reports
about 104
run entitlement report 105
request password release 121
request workflow
audit 102
dialog 142
password release requests 120
Requester tab 279
reset bootstrap admin password 552
reset cluster 497
resolve IP address in managed networks 374
restart appliance 319, 552

restore
backup file 353
clustered appliance 495
review
password release request 127
session access request 141
session release request 141
Reviewer tab 282
role-based access control 507
role-based email notifications 119
run
account discovery setting 235
run asset discovery job 190
run entitlement report 105
run in the system tray 85

S

Safeguard
features 27
set up 68
Safeguard Access settings 435
Login Control 436
Time Zone 442
User Password Rules 438
Safeguard PowerShell 53
SAP HANA
prepare for Safeguard 529
SAP Netweaver Application Servers
prepare for Safeguard 529
save search criteria 97
schedule
activity audit log report 99
asset discovery 245
auto account password reset 427
auto account password validation 430
backup, how to 350
scope
add assets or accounts to partition 301
Scope tab
partition 295-296
search box 111
using 111-112
secondary authentication
about 457
enable 455
login 82
Secret Key, about 211
Security Policy Administrator permissions 516
separation of duties 68
server
archive, configure 345
service account 147
about 201
set as managed account 201
service discovery
how to setup 251
session access request 129
approve 137
check-in session 133, 135
launch RDP session 139
launch session 133, 135
launch SSH client 138
review 141
revoke 138
session module password access enabled
disable 312
enable 312

session recording
about 128
follow mode 143
play back 142
Session Recording Signing Certificate 356
session release
checkout 133, 135
session release request
cancel pending request 134, 136
remove request 134, 136
review 141
session request workflow 128
session requests
disable 310
enable 310
Session Settings tab 285
sessions
about 128
about certificates 356
sessions certificates
about 356
sessions management
about 377
set account password reset schedule 427
set account password validation schedule 430
set appliance name 318
set appliance system time 571
set password
generate 165, 565
manual 166
set telnet, 3270, and 5250 session access requests 569
settings
Access Request 309
Account Discovery 248
Account Password Rules 421
Appliance 313
Appliance Diagnostics 59, 315
Appliance Information 313, 315
Application to Application 382
Approval Anywhere 393
Archive Servers 344
Asset Management 332
Audit Log Signing Certificate 356
Autit Log Management 346
Backup and Retention 343
backup settings 350
Certificate Signing Request 359
Certificates 355
Change Password 425
Change Password Management Enabled 311
Check Password 429
Check Password Management Enabled 310
Cluster 365
Cluster Management 366
custom platforms 333
desktop client application settings 84
Diagnostics 323
Email 395
Enable Backup Retention 354
Enable or Disable Services 309, 319
External Federation 561
External Integration 381
Factory Reset 320
Licensing 321
Lights Out Management (BMC) 322
Login Control 436
Login Notification 420

Managed Networks 369
Message of the Day 420
Messaging 420
Networking 326
Password Requests Enabled 310
Profile 421
Reasons 312
run in the system tray 85
Safeguard Access 435
Safeguard Backup and Restore 348
Safeguard Retention 354
Session Module Password Access Enabled 312
Sessions Certificates 356
sessions management 377
SNMP 411
SSL Certificates 360
Starling 412
Support Bundle 330
Syslog 415-416
Tags 335
Ticketing 418
Time 330
Time Zone 442
Trusted Certificates 363
User Password Rules 438
setup Safeguard 68
setup Starling account 413
show ignored assets 148, 180
show routes 326
shut down appliance 318
shutdown appliance 552
sign up for Starling One Identity Hybrid service trial account 413
SNMP
copy subscription 411
delete subscription 410
modify subscription 410
SonicOS devices
prepare for Safeguard 531
SonicWALL SMA or CMS appliances
prepare for Safeguard 531
sort entity lists 114
sorting report results 103
SSH Host Key
add 542
algorithms for key exchange 542
SSH Host Key Fingerprint
About 184
SSH key
download 222
import 205
SSH session
launch SSH client 138
SSL certificates
about 360
assign to appliance 363
create certificate signing request 362
install 362
SSL support
about 571
Microsoft SQL servers 572
MySQL servers 573
Sybase ASE servers 574
Starling join 412
Starling One Identity Hybrid service
setup account 413
start desktop client 82
support bundle 330, 554
supported platforms 37

Sybase ASE servers
prepare for Safeguard 530
SSL support 574
syslog 415
configure 416
copy server configuration 416
delete server configuration 416
modify server configuration 416
system requirements 34
desktop client 35
web client 36
web management console 37

T

tags
copy asset or asset account tag to another partition 342
delete asset or asset account tag 341
manage asset and asset account tags 335
manually adding a tag to an account 159
modify asset or asset account tag 341
view asset and asset account tag assignments 342
when does rules enginer run 577
tasks
stop 146
viewing 145
telnet
certificate support 521, 525, 528, 534
session access request setup 569
Telnet 325
terminate session play back 143
Test Connection
about 202
disable UAC to resolve connectivity failures 540
resolve failures 555
ticketing system
delete 419
integrate with Safeguard 418
modify settings 419
time
current appliance time 330
time restrictions 276
Time Restrictions tab
Access Request Policy dialog 286
Entitlement dialog 275
time zone
configure 442
timeout errors causing operations to fail 558
timestamp
conversion 106
Timestamping Authority Certificate 356
TLS 1.2 setting 315
toast notifications 118
about 85
toolbar
Adminitrative Tools views 109
main screen 84
Toolbox
about 145
Topic Secret - Mainframe systems
prepare for Safeguard 533
trace route 325
troubleshooting
account is stuck in a pending password change state 548

account is stuck in a pending password review state 547
appliance information 551
appliance status 544
cannot add replica to cluster 554
cannot connect to remote machine through SSH or RDP 543
Check Password fails on Unix host 422, 547
Check, Change, or Set failures 540
cluster 501
diagnostic tests 323
domain controller issues 557
error message
- An internal request has timed out 554
- Anti Cross Site Request Forgery token error 540
- cannot play session 544
- no cipher supported 542
- No SSH host key was provided 540
- system was unable to unlock your login keychain 546
- There is no cipher supported by both client and server 556

factory reset 553
How do I access the recovery kiosk 549
How do I close a password request without review 547
How do I dowload MIB Definitions 411
How do I enable Network Time Protocol (NTP) 331
How do I generate a support bundle 554
How do I make a Safeguard SSL Webserver Certificate 362
How do I move assets from one partition to another 213
How do I obtain a new password during an open request 578
How do I reassign assets from one partition to another 302
How do I reboot the appliance 552
How do I reset the bootstrap admin password 552
How do I set a directory account's time zone 474
How do I shut down the appliance 552
How do I test an asset's connectivity 212
incorrect or insufficient service account privileges 542
incorrect service account credentials 541
incorrect SSH host keys 541
login credentials fail on Unix host 422, 547
networking issues 558
password fails for Unix host 547
Safeguard is not working on Windows-based systems 558
Test Connection fails for admin account on Windows machine not in domain 540
Test Connection failures 540, 555
Test Connection failures on archive servers 556
Test Connection failures on assets that require SSL 556
timeout errors causing operations to fail 558
What do I do if the system services do not restart 555
Why are directory users in wrong time zone 456

Why are my email template marcros blank 398
Why can't I checkout an account 548
Why can't I delete an account 547
Why can't my AD user log in 544
Why did Test Connection fail 540, 556-558
Why did the password change fail 160, 202, 540, 543
Why didn't a user receive email notifications 396
Why didn't the automatic password check and change run on schedule 548
Why doesn't Safeguard automatically Check and Change SSH Keys 203
Why don't others see the changes I made 109
Why is the bootstrap account locked out of Safeguard 559
Why is the user account locked out of Safeguard 559
Why isn't the password available for checkout 202, 547-548
Why wasn't the Approver (or reviewer) notified 559
troubleshooting tools 313
trusted certificates
about 363
add 364
remove 364

U

uninstall desktop client 83
Unix-based systems
prepare for Safeguard 534
unjoin
cluster member 484
unlock account 466
unlock locked cluster 501
update license file 321
update Safeguard appliance 332
updates
install 332
user
about 443
add 444, 451, 564
add from Users selection dialog 288
add to entitlement 288, 448, 461
add to group 477
add to user group 446, 459, 476
administrator permissions 456
authentication settings 453
change password 86
change personal contact information 86
change photo 86
change time zone 461
delete 444
enable or disable 461
Entitlements tab 447
export history 450
General tab 444
grant partition ownership 461
import 444
Linked Accounts tab 448
modify 461
Partitions tab 446
remove 462
reset password 465
User Groups tab 446

view history 450, 461
User Administrator permissions 517
User dialog
Authentication tab 453
Permissions tab 456
user group
about 467
add 459, 473
add from User Groups selection dialog 288
add member 446, 459, 468, 476
add to entitlement 288, 477
add to role 478
add user 446, 459, 468, 476-477
change description 477
delete 467
Entitlements tab 469
General tab 468
History tab 471
modify 477
remove 478
Users tab 468
User Groups tab
user 446
user password rule
about 438
configure 439
Users tab
entitlement 268
user group 468

V

view
access request details 93
account discovery setting 235, 249
activity event details 102
asset and asset account tag assignments 342
Check and Change Log 154
custom platform 333
virtual appliance 55
backup and recovery 57, 66
set up 42
virtual kiosk
support kiosk 58
VMware
backukp and recovery 57, 66
VMware ESXi Hosts
prepare for Safeguard 522

W

web client 72
about 84
approvals 75
change password 78
favorites 76
FIDO2 keys 79
log out 79
my requests 74
reviews 76
settings 77
system requirements 36
version 77
Windows client 77
web management console 55
system requirements 37
widgets
administrator widget 547
approvals widget, controls 126, 137
requests widget, controls 135

reviews widget, controls 127, 141
Windows systems
minimum required permissions 536
prepare for Safeguard 535, 538