One Identity Safeguard for Privileged Passwords 2.7

Evaluation Guide

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Safeguard for Privileged Passwords Evaluation Guide
Updated - May 2019
Version - 2.7

Contents

1

Introduction

The One Identity Safeguard for Privileged Passwords Evaluation Guide steps you through a self-directed, hands-on demonstration of the core features of Safeguard for Privileged Passwords and will enable you to perform a POC (proof of concept) of its capabilities in your own test lab

Introduction to One Identity Safeguard for Privileged Passwords

The One Identity 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 timeframe to value.

Safeguard privileged management software suite

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

The Safeguard products' unique strengths are:

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

The suite includes the following modules:

- **One Identity Safeguard for Privileged Passwords** automates, controls and secures the process of granting privileged credentials with role-based access management and automated workflows. Deployed on a hardened appliance, 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 - integrating 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.

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. Two types of access may be granted to assets 1) passwords (including secrets) and 2) sessions.

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 users 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.

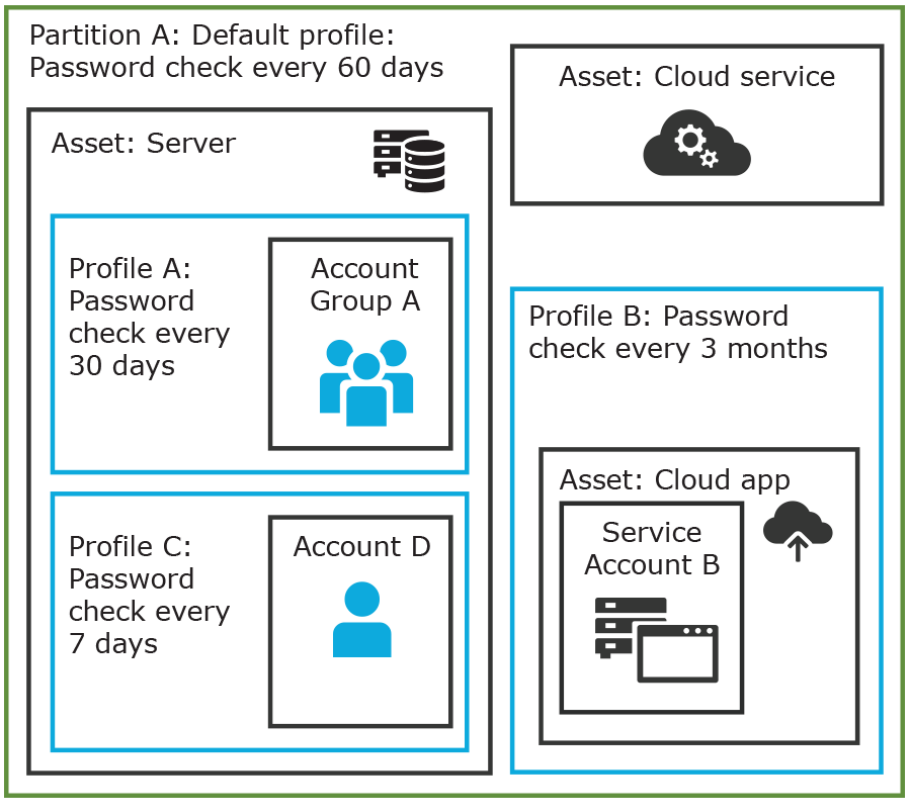
An asset can be assigned to only one partition at a time. When you assign an asset to a partition, all accounts associated with that asset are automatically reassigned to that partition, as well. Then, any new accounts you add for that asset are automatically assigned to that partition.

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 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 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 7 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 7 days.



In the example above, 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 3 months, and Profile C has the highest level of security, checking passwords every 7 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.

Details: Assets and asset groups

- An asset may be a computer, server, network device, directory, or application.
- You can log into 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.

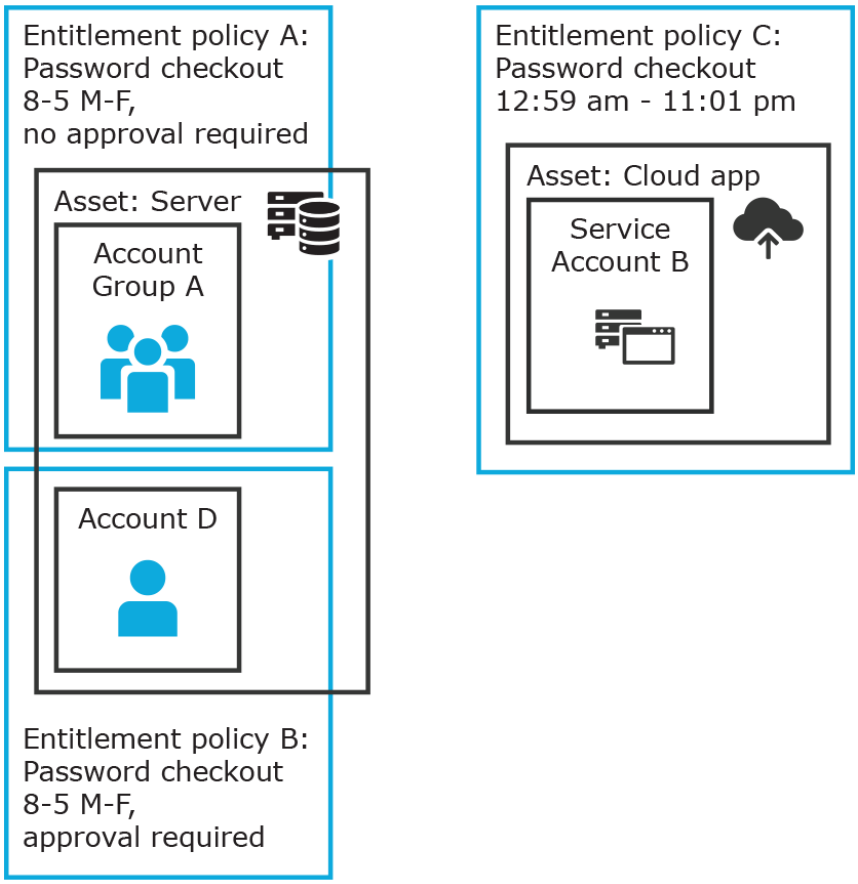
Entitlements grant access to users, user groups, or both. An entitlement includes one or more access request policies and may be related to job functions like help desk support or Unix administrators.

An entitlement access request policy defines what is managed by the policy and is referred to as the "scope of the policy". There are two types of access requests: password and sessions.

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

Entitlement access request policies may include:

- The access type: Password or sessions which include SSH or RDP (remote desktop)
- The scope: Accounts, account groups, assets, and asset groups as needed
- Requestor settings: For example, reason for the request, comment, ticket number, and access duration
- Approver and Reviewer settings: If required, the approvers and reviewers along with notifications
- Access configuration: Settings based on the type of access (Password, SSH, or RDP set earlier)
- Session settings: If used, record sessions
- Time restrictions: If used, days and hours of access
- Emergency settings: If used, who to contact



In the example above, 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 am to 5 pm Monday through Friday with no approval required. Entitlement access request policy B, which is associated with Account D, allows for password checkout for the same time frame but the checkouts require approvals. Entitlement access request policy C allows for password checkout from 12:59 am to 11:01 pm to allow for the system maintenance window.

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 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 authorized 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, SSH, 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 other conditions. 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, Policy Administrator, User Administrator, and Auditor should be different users.

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

Users can be configured for two-factor authentication.

Details: Users and user groups

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

Discovery

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

Password request high level workflow

1. A user or service requests the password of an account.
2. Based on the entitlement access request policy, the password is automatically granted or the password request can be sent through an approval process. The workflow can also include a reviewer to review all access activities for legitimacy.
3. The session launches on a machine or via a graphical user interface such as SSH or RDP (Remote Desktop Protocol).

Passwords can be checked in or are otherwise valid for the duration of the request. Safeguard resets the password and passwords are constantly changing to monitor and audit access to assets.

Session access

Session access and activities are proxied through Safeguard and are captured in audit logs. Session activities at the screen and keystroke level can be captured, viewed, and used for forensic audits.

Key features

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

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 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.

Feature	Description

Directory integration	You can leverage your existing directory infrastructure (such as Microsoft Active Directory). You import import directory users and directory groups. Directory users authenticate to Safeguard for Privileged Passwords with their directory credentials.
	
	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

Feature	Description

	• 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.
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 uses a modernized API based on a REST architecture which allows other applications and systems to connect and interact with it. The API enables quick and easy integration with diverse systems and applications spanning many programming languages.
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

Feature	Description
	to Safeguard for Privileged Passwords. Safeguard for Privileged Passwords supports any Radius-based 2FA solution and One Identity's Starling Two-Factor Authentication service.
Workflow engine	A 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. An access request can be automatically approved or require multiple sets of approvals.

Sessions key features

To record and playback sessions, you may use one of the following methods:

- The embedded sessions module that comes with Safeguard for Privileged Passwords.

  CAUTION:The embedded sessions module in Safeguard for Privileged Passwords version 2.7 will be removed in a future release (to be determined). For uninterrupted service, organizations are advised to join to the more robust Safeguard for Privileged Sessions Appliance for sessions recording and playback.

- 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* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Table 2: Key features using sessions

Command detection	During a privileged session, commands that are being run on the target host are detected. All actions are logged and can be sent out, if configured, to various logging mechanisms (syslog, email, SNMP). NOTE: For an RDP session, Safeguard for Privileged Passwords can detect the title of any window that is opened on the desktop during a privileged session.
Full session audit, recording and replay	With sessions, every packet sent and action that takes place on the screen -- including mouse movements, clicks and keystrokes -- is recorded and available for review. The time and content of the session are cryptographically signed for forensics and compliance purposes. Only actual activity is recorded, and recordings are compressed to a fraction of the size required by other solutions to minimize offline storage requirements.

Indexing	With sessions, you can create a searchable list of commands and programs that were run during the recorded session. Auditors have a quick and easy view to session activities.
Protocol support	The embedded sessions module provides full support for the SSH and RDP protocols. In addition, administrators can decide what options within the protocols they want to enable/disable.
Proxy access	All sessions are proxied to target resources. Since users have no direct access to resources, the enterprise is protected against viruses, malware, and other dangerous items on the user's system. The embedded sessions module can proxy and record Unix/Linux, Windows, network devices, firewalls, routers and more.
Work the way you want	Sessions enables administrators to choose their access tools and tool preferences (for example, PuTTY) when gaining access to privileged sessions. This creates a frictionless solution that gives administrators the access they need while meeting compliance and security regulations.

What's new in version 2.1

One Identity Safeguard for Privileged Passwords 2.1 introduces the following new features and enhancements.

Table 3: Safeguard 2.1: Features and enhancements

Feature/Enhancement	Description
Additional platform support	Safeguard for Privileged Passwords now supports the management of assets on the following additional platforms: • ACF2 - Mainframe r14 and r15 • ACF2 - Mainframe LDAP r14 and r15 • Debian GNU/Linux 9 • ESXi 6.5 • Fedora 26 • Fortinet FortiOS 5.2 and 5.6 • F5 Big-IP 12.1.X and 13.0 • MAC OS X 10.13
Cluster patching	The cluster patching process now allows you to patch all cluster members without having to first unjoin a replica and re-enroll it after it has been updated. During the cluster patch operation, access request workflow is available so authorized

Feature/Enhancement	Description
	users can request password releases and session access.
Federated login	One Identity Safeguard for Privileged Passwords supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different Identity Provider STS servers and services, such as Microsoft's AD FS.
Immediate recording archival	One Identity Safeguard for Privileged Passwords provides the ability to immediately archive session recordings from a specific Safeguard for Privileged Passwords Appliance to a specified archive target. When an archive server is configured, session recordings are removed from the Safeguard for Privileged Passwords Appliance and stored on the archive server.
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 enables the Appliance Administrator to power on an appliance remotely or to interact with the recovery kiosk.
Multi-request	Authorized Safeguard for Privileged Passwords users can now request multiple password releases or sessions in a single request. In addition, these requests can be saved as a "favorite" access request, providing quick access to the request from the user's Home page.
Safeguard for Privileged Passwords Desktop Player enhancements	The new version of the Safeguard for Privileged Passwords Desktop Player includes the following new features: • Ability to display user activity as subtiltes when playing back a recorded session. The user activity that can be displayed as subtitles includes windows titles, executed commands, mouse activity, and keystrokes, as they occurred during the recorded session. • New timeline with user event indicators showing when user activities and screen changes occurred within the recorded session. Clicking an indicator on the timeline takes you to the relevant user event in the recording. • Ability to export the sessions recording file, including the user event subtitles, as a video file.
Security Policy Administrator dashboard	The new Access Request dashboard allows Security Policy Administrators to review and manage access requests from a single location. From this view, the Security Policy Administrator can revoke a request, follow an active session, or terminate a session.

Feature/Enhancement	Description
Restore/Suspend accounts	Safeguard for Privileged Passwords allows you to suspend Safeguard for Privileged Passwords managed accounts when they are not in use to reduce the vulnerability of password attacks on privileged accounts. NOTE: This new feature applies to Windows platforms (Windows server and Active Directory accounts) and Unix platforms (AIX, HP-UX, Linux, Solaris, and Mac OS X accounts).
TLS 1.2 Only	To remediate security vulnerabilities identified in early versions of the TLS encryption protocol, Appliance Administrators can configure Safeguard for Privileged Passwords to respond only to TLS 1.2 requests. This allows organizations to comply with the security and strong cryptography requirements in PCI-DSS.
X11 Forwarding	When configuring the settings for SSH session access requests, Security Policy Administrators can now enable **Allow X11 Forwarding**, which forwards a graphical X-server session from the server to the client.

What's new in version 2.2

One Identity Safeguard for Privileged Passwords 2.2 introduces the following new features and enhancements.

Table 4: Safeguard for Privileged Passwords 2.2: Features and enhancements

Feature/Enhancement	Description
Additional platform support	Safeguard for Privileged Passwords now supports the management of assets on the following additional platforms: • FreeBSD • MongoDB • PostgreSQL • RACF - Mainframe LDAP • SAP HANA
Application to Application (A2A) integration	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

Feature/Enhancement	Description
	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.
Asset administrator dashboard	The **Account Automation** tab on the **Dashboard** allows Asset and Directory administrators to view information regarding accounts that are failing different types of tasks, including: • Accounts where password check tasks failed. • Accounts where password change tasks failed. • Accounts where SSH key change tasks failed. • Accounts where suspend tasks failed. • Accounts where restore tasks failed.
Dynamic grouping and tagging	Dynamic grouping and tagging helps classify assets allowing Safeguard for Privileged Passwords to assign automatically provisioned systems and accounts to a policy. Tags allow Asset administrators to add additional metadata to accounts and assets to enrich the data on the object as it is added to Safeguard for Privileged Passwords. Tags can be dynamically added to assets and accounts based on tagging rules or they can be added manually. Policy administrators can create rules based on tags or from attribute information that is on the account or asset (for example, name, platform, partition, network address, and so on) to define group membership.
Event subscription	As a Safeguard for Privileged Passwords user, you can now control the email notifications you receive. Using the **Manage Email Notifications** control in your **My Account** pane, you can remove the events for which you do not want to receive email notifications. As a Safeguard for Privileged Passwords administrator, you can use the API to subscribe to the events for which you are interested in receiving notifications.

Feature/Enhancement	Description
Audit log archive	Safeguard for Privileged Passwords allows you to define and schedule an audit log management task to rotate audit logs from the Safeguard for Privileged Passwords appliance and archive older audit logs to a designated archive server.
Site awareness and network segmentation	As an Appliance administrator, you can define managed networks (network segments) for your organization so Safeguard for Privileged Passwords can more effectively manage assets and accounts, and service access requests. Managed network information is used for scheduling tasks, such as password change and account discovery, and for session management in a clustered environment to distribute the task load. That is, by using managed networks the load is distributed in such a way that there is minimal cluster traffic and appliances that are closest to the target asset are used to perform the task.
Attribute search	The attribute search functionality in the user interface allows you to limit an object list based on the object attributes. For example, in the Accounts view, you can now filter the accounts list based on whether the specified attribute contains the search string entered.
Starling Join	The newest versions of One Identity's on-premises products offer a mandatory One Identity Hybrid Subscription, which helps you transition to a hybrid environment on your way to the cloud. The subscription enables you to join Safeguard for Privileged Passwords with the One Identity Starling software-as-a-service platform. This gives your organization immediate access to a number of cloud-delivered features and services, which expand the capabilities of Safeguard for Privileged Passwords. When new products and features become available to One Identity Starling, the One Identity Hybrid Subscription allows you to use these immediately for Safeguard for Privileged Passwords to add value to your subscription.
Starling Identity Analytics & Risk Intelligence integration	The Starling Identity Analytics & Risk Intelligence service collects and evaluates information from data sources, such as Safeguard for Privileged Passwords, to provide you with valuable insights into your users and entitlements. When integrated with Safeguard for Privileged Passwords, Starling Identity Analytics & Risk Intelligence allows you to identify Safeguard for Privileged Passwords users and entitlements that are classified as high risk and view the rules and details attributing to that classification.

What's new in version 2.3

One Identity Safeguard for Privileged Passwords 2.3 introduces the following new features and enhancements.

Table 5: Safeguard for Privileged Passwords 2.3: Features and enhancements

Feature/Enhancement	Description
Synchronized passwords	As an Asset Administrator, you now have the ability to synchronize passwords so accounts can use the same password on the same or different assets.

What's new in version 2.4

One Identity Safeguard for Privileged Passwords 2.4 introduces the following new features and enhancements.

Custom platform (770747)

Asset Administrators now have the ability to add a custom platform for use when adding or updating an asset. A custom platform allows Safeguard for Privileged Passwords to connect to and manage password operations on platforms that are not supported by Safeguard for Privileged Passwords out of the box. You can upload a custom platform script file to add support for any system that you want to manage. In this release, only SSH-based custom platforms are supported; other protocols will be added in future releases. To access examples of custom scripts and view commands, visit:

- Scripts:

  https://github.com/OneIdentity/SafeguardCustomPlatform
- Command wiki:

  https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Command-Reference

Auditors and Partition Administrators have read only rights to custom platforms. However, Partition Administrators retain the ability to add or remove assets.

Authentication options (765396)

With appropriate administration credentials, you can change the primary and secondary identity and authentication providers for authentication to Safeguard for Privileged Passwords. The feature enables customers to integrate Safeguard for Privileged Passwords with their existing identity and authentication services. For example, a customer can use Radius for primary authentication and rely upon their own company policies for functions like 2FA.

Safeguard Sessions Appliance join (770739)

CAUTION: The SPS/SPP join feature in the Safeguard for Privileged Passwords 2.4 release is intended for proof of concept and preview purposes only. This feature should not be used in production.

The Asset Administrator can now join a Safeguard Sessions Appliance with a standalone primary Safeguard for Privileged Passwords Appliance. Once joined, all sessions are recorded via the Safeguard Sessions Appliance and the embedded sessions module for Safeguard for Privileged Passwords is no longer available.

The user initiates the join by connecting to the Safeguard Sessions Appliance over SSH, selecting **Join to SPP**, and providing the requested information. After the join is complete, the user restarts the desktop client to complete the connection and update settings and entitlement policy details.

Sessions recorded prior to joining the Safeguard Sessions Appliances are available to play back from local storage and in accordance with the permissions of the Safeguard for Privileged Passwords Appliance. Sessions that are archived are also available to play back.

Once a Safeguard for Privileged Passwords Appliance has been configured to use the Safeguard Sessions Appliance, it can only be reversed by a factory reset of the Safeguard Passwords Appliance or restoring a backup that was taken before the first join of Safeguard for Privileged Sessions (SPS). Either method unjoins the Sessions Appliance and redeploys the Safeguard for Privileged Passwords Appliance sessions module.

What's new in version 2.5

One Identity Safeguard for Privileged Passwords 2.5 introduces the following new features and enhancements.

Directory based user discovery (713614 and 761638)

When adding a new directory based user group, the Authorizer Administrator or the User Administrator now have the option to:

- Configure primary and secondary authentication providers and
- Set administrator permissions on the imported or updated Safeguard for Privileged Passwords users.

In addition, any managed directory accounts that exist in Safeguard for Privileged Passwords at the time of the import process (or during the background synchronization of the directory), can automatically be assigned to a Safeguard user as a linked account. That association will be dependent upon the value of an attribute from the directory (such as "managedObjects" or "directReports" in Active Directory or "seeAlso" in OpenLDAP 2.4).

Offline Workflow (782735)

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 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 manually resume online operations to merge audit logs, drop any in flight access requests, and return the appliance to full participation in the cluster.

It is recommended that no changes to cluster membership are made while an appliance is in Offline Workflow Mode. The Appliance Administrator must manually restore the online operations before adding other nodes to ensure the appliance can seamlessly reintegrate with the cluster.

What's new in version 2.6

One Identity Safeguard for Privileged Passwords 2.6 introduces the following new features and enhancements.

Automatic Offline Workflow Mode (794644)

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 5 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 5 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.

This new feature is available via **Settings** | **Cluster** | **Offline Workflow**.

Export a report as a .csv or .json file (788932)

Administrators and users can export a report to a .csv or .json file to easily view, manipulate, and share data. This functionality includes entitlement reports, Activity Center exports, Activity Center scheduled reports, account automation reports, and access request reports.

Identity provider initiated single sign on flow (788935)

To enable users to have a centralized logon experience, an Appliance Administrator can configure their identity provider to redirect to Safeguard for Privileged Passwords. All security requirements, such as two-factor authentication, are enforced. For example, a user can go to a portal, authenticate against their identity provider, and select an application, including Safeguard, based on their organizational role. Safeguard accepts the "unsolicited" SAML 2.0 response assertion and logs in the user without additional authentication.

Systems Integrators can offer Safeguard as an application in their single sign-on (SSO) portal. Support personnel can then click the appropriate tool on their dashboard to access Safeguard for Privileged Passwords and Safeguard for Privileged Sessions.

This feature only works with SAML 2.0 and the web user interface, not the desktop client.

Policy allows password requests to include all linked accounts (776867)

A Policy Administrator can create a policy that allows a user's password request to include access to assets for all the accounts linked to the user's account. For example, if a company uses personal admin accounts in Active Directory, a single policy can be created to grant password access to each user with a personal admin account.

This function is set by selecting the following check box: **Entitlements** | **Access Request Policy** | **Access Config** | **Allow password access to linked accounts**.

Restore a backup from a previous version (790917)

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.

Service discovery (773722)

Overview

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

Service discovery jobs run automatically in the background or may be manually run.

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 on the **Partitions** | **Discovered Services** tab as **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 linked to the asset with the account managed by Safeguard. Effectively, the asset will have an account dependency on the account.

To automatically link, the Account Discovery job (which runs when Safeguard synchronizes the directory) must have the **Automatically Manage Found Accounts** check box selected on the Discovery tab. The **Directories** | **General** tab designates the directory profile to govern the accounts the discovery job adds to Safeguard.

Unmanaged accounts

The administrators can view the Partitions | Discovered Services tab to identify unmanaged accounts that they may want to manage to require authentication for local users or Active Directory users, if the asset is joined to a domain. For more information, see Adding an account.

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**.

Session player installation (794597)

> **CAUTION: To play back sessions, the new Desktop Player must be installed for one user or system-wide users after installing Safeguard for Privileged Passwords 2.6.**

When Safeguard for Privileged Passwords 2.6 is installed, the existing Desktop Player is removed and the latest Desktop Player must be installed.

Once Safeguard for Privileged Passwords is installed, the new player can be accessed by going to the Windows **Start** menu, **Safeguard** folder and clicking **Download Safeguard Player**. The One Identity Safeguard for Privileged Sessions - Download Software web page displays.

To continue the installation for one or system-wide users, follow the *Install Safeguard Desktop Player* section of the player user guide found here:

1. Click this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.
2. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.

User experience if the Desktop Player is not installed

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** and will be taken to the download page to complete the install.

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.

Time zone change (780266)

Safeguard for Privileged Passwords sets a default time zone based on the location and culture 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 am to 5 pm). It is recommended that the Bootstrap Administrator set the desired time zone on set up. A User Administrator can also change the time zone.

Time zone changes are made via **Settings** | **Safeguard Access** | **Time Zone** and selecting the **Default User Time Zone**.

What's new in version 2.7

One Identity Safeguard for Privileged Passwords 2.7 introduces the following new features and enhancements.

Sessions Appliance join (792394)

> **CAUTION: The embedded sessions module in Safeguard for Privileged Passwords version 2.7 will be removed in a future release (to be determined). For uninterrupted service, organizations are advised to join to the more robust Safeguard for Privileged Sessions Appliance for sessions recording and playback.**

Managing sessions via the Safeguard Sessions Appliance is now available for use in production. For this release, the embedded sessions module for Safeguard for Privileged Passwords is still available.

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.

Session recording, playback, and storage

- 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.

Safeguard for Privileged Passwords join guidance

Before initiating the join, review the steps and considerations in the join guidance. For more information, see *Safeguard for Privileged Passwords Administration Guide*, Appendix C: SPP and SPS sessions appliance join guidance.

Safeguard for Privileged Sessions join steps and troubleshooting

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* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Separate identity and management for directories for fine grained management (773267)

The following information summarizes the changes at a high level. For more information specific for your initial deployment of Safeguard for Privileged Passwords 2.7, see the *Safeguard for Privileged Passwords Administration Guide*, Appendix B: SPP 2.7 Migration guidance.

Overview

Safeguard for Privileged Passwords version 2.7, has been 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, 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.

The following information details the changes from version 2.6 to version 2.7. The same information is generally true if you are upgrading from version 2.1 forward to version 2.7.

Administrators

- 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.

Identity

During the migration to version 2.7, directories are migrated as an asset with the appropriate identity provider and associated users.

Management

Directories can be subdivided so administrators can be assigned to manage portions of a directory. For example, Admin A might only manage objects in the Finance organizational unit (OU) of the directory and Admin B might 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.

Accounts

- You can select a directory account and view the assets that have a dependency on the account.
- You can sync passwords between a directory account and an asset account.

Assets

- Directories are migrated to assets with the appropriate provider assignment.
- Directories are still synced with Safeguard.
- Migrated directory assets reflect the account dependencies.
- You can select whether a directory asset manages the forest or a subset of the forest. Multiple assets be assigned against the same forest.

- Migrated directory assets are available for access discovery jobs beyond partition boundaries.
- Each migrated directory asset is assigned to its own partition and includes the Account Discovery schedules, the check and change schedules, account password rules, password sync groups, and related functions.
- A directory is a member of an asset partition so that ownership of different parts of the directory can be delegated.
- During import, entities imported from a directory must be unique across all partitions (for example, you cannot import Admin C account into multiple asset partitions).
- When you add an asset, the Account Discovery schedule for the partition is displayed and can be changed.

Discovery schedules

- Account discovery includes the option for discovered accounts: enable password requests, enable session requests, and make the discovered accounts available for use across all partitions.
- Account discovery can be configured as Unix based, Windows based, or Directory based, each with its own schedule.

Account discovery enhancements (788930)

Asset Administrators and delegated partition owners can create account discovery jobs to perform the functions in the following list:

- Set the default password of a discovered account to configure the environment initially and incrementally.
- Add a discovered account to a sync group to configure the environment initially and incrementally.
- Immediately check and change the password of discovered accounts that are set to be automatically managed. This places the account under immediate management rather than waiting for the schedule to execute.

> NOTE: In **Settings** | **Profile**, the partition profile's **Change Password Schedule** and **Check Password Schedule** must both be set to a value other than **Never**.

Activity Center enhancements (799288, 799308, 799307)

From the Activity Center, you have the option to choose All entities (such as users, assets, and accounts) without picking all of them. You can export the report without first previewing the report.

Allow Oracle SYS account as a service account (799993, 800128)

An Asset Administrator responsible for Oracle database servers can use the SYS account with either SYSDBA or SYSOPER system privileges as a service account.

The SYS account is automatically created when the administrator installs Oracle and has the necessary privileges. See the Oracle document, About Administrative Accounts and Privileges, for more information. The SYS user is automatically granted the SYSDBA privilege on installation and can be SYSOPER. For more details, see the Oracle document, SYSDBA and SYSOPER System Privileges.

This is set via setting the Service Name when you add or edit an asset. Navigate to **Administrative Tools** | **Assets** | **Connection** tab.

Asset discovery enhancements (782848)

Asset Administrators are now given:

- Expanded connection options when setting up the connection template to discovered assets to automatically manage discovered assets and service accounts.
- The ability to set a platform type in the asset discovery rules.
- The ability to assign a different profile to service accounts in the asset discovery rules so that the service account is assigned a profile other than default asset profile inherited by other accounts discovered on the asset.

In addition, SSH keys are now auto-accepted for supported platforms.

Custom platform: TN3270 (798892)

An Asset Administrator responsible for an AS400 and mainframe infrastructure (such as ACF2 or RACF) can manage servers customized log in screens and connection strings.

A custom platform author can create a customer platform script to check and change passwords against servers where the login screens and connection strings have been customized.

Microsoft SQL Server TCP/IP support (798894, 799577)

An Asset Administrator responsible for Microsoft SQL Server can have Safeguard for Privileged Passwords connect to the databases using TCP/IP rather than named pipes.

Multiple directory account session support with access request policy (792426)

A Policy Administrator can add multiple directory accounts to a single access request policy. For example, you can grant access to a Windows asset via RDP using one of multiple directory accounts. Accounts are added when you create or edit an access request policy via the **Administrative Tools** | **Entitlements** | **Access Request Policies** | **Directory Account** option.

Radius enhancements (798896)

The User Administrator is offered two new configuration controls on **Settings** | **External Integration** | **Identity and Authentication** when Radius is selected as the provider.

- The User Administrator can choose to mask the Radius secondary authentication response entered by users by selecting the **Always Mask User Input** check box. 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 just 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.
- The User Administrator can choose to have the Radius secondary authentication pre-submit an Access-Request message to the Radius server in order to initiate a challenge/response cycle before the user sees or enters any information. The **PreAuthenticate for Challenge/Response** check box is used to indicate whether an Access-Request call containing only the User-Name should be 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 the server 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. Note, 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.

In addition, the timeout for log in is now configurable to more than 60 seconds.

Setting up Safeguard for Privileged Passwords

By following these procedures you will set up a hierarchy of administrators that ensures your company follows entitlement-based access control, as you step through the process of writing some basic policies.

- Setting up the appliance
- Creating local administrator users
- Configuring external integration settings
- Creating local users
- Adding assets and accounts
- Writing entitlements

NOTE: To streamline your software evaluation, these instructions are not detailed. For a full explanation of the features, refer to the *One Identity Safeguard for Privileged Passwords Administration Guide*.

Setting up the appliance

Follow these steps to set up and configure the One Identity Safeguard for Privileged Passwords 2000 Appliance.

Step 1: Before you start

1. Ensure that you install the Microsoft .NET Framework 4.6 (or greater) on your management host.

Step 2: Prepare for installation

Gather the following items before you start the appliance installation process:

1. Laptop
2. IP address
3. IP subnet mask
4. IP gateway
5. DNS server address
6. NTP server address

   NOTE: If a Safeguard for Privileged Passwords Appliance is going to be used for both Privileged Passwords and the sessions module, you need this network interface information for both the appliance and the embedded sessions module.

   CAUTION:The embedded sessions module in Safeguard for Privileged Passwords version 2.7 will be removed in a future release (to be determined). For uninterrupted service, organizations are advised to join to the more robust Safeguard for Privileged Sessions Appliance for sessions recording and playback.

7. One Identity Safeguard for Privileged Passwords license.

   If you purchased One Identity Safeguard for Privileged Passwords, the appropriate license files should have been sent to you via email. If you have not received an email or need it to be resent, visit https://support.oneidentity.com/contact-us/licensing. If you need to request a trial key, please send a request to sales@oneidentity.com or call +1-800-306-9329.

   NOTE: One Identity Safeguard for Privileged Passwords ships with the following modules, each requiring a valid license to enable functionality:

   - Privileged passwords
   - Embedded sessions module

Step 3: Rack the appliance

Prior to installing the racks for housing the appliance, refer to the Warnings and precautions appendix in the *One Identity Safeguard Appliance Setup Guide* provided in the box with the hardware equipment.

Step 4: Power on the appliance

Prior to powering up the appliance, see the Standardized warning statements for AC systems appendix in the *One Identity Safeguard Appliance Setup Guide*.

The One Identity Safeguard for Privileged Passwords 2000 Appliance includes dual power supplies for redundant AC power and added reliability.

1. Plug the power cords to the power supply sockets on the appliance back and then connect the cords to AC outlets.

   TIP: As a best practice, connect the two power cords to outlets on different circuits. One Identity recommends using an UPS on all appliances.

2. 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 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.

   You can use the **Red X** button to shut down the appliance. Once the Safeguard for Privileged Passwords Appliance is booted, press and hold the **Red X** button for four seconds until it displays POWER OFF.

   NOTE: If the Safeguard for Privileged Passwords Appliance is not yet booted, it may be necessary to press the **Red X** button for up to 13 seconds.

   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.

Step 5: Connect the management host to the appliance

The port used for a secure first-time configuration of the appliance is **MGMT**. This IP address is a fixed address that cannot be changed. It will always be available in case the primary interface becomes unavailable. The **MGMT** IP address is: 192.168.1.105.

The "primary interface" that connects your appliance to the network is **X0**. You must change the primary interface IP to match your network configuration. The default **X0** IP is: 192.168.0.105.

IMPORTANT: The appliance can take up to five minutes to boot up. In addition, ping replies have been disabled on the appliance, so you will not be able to ping this secure appliance.

1. Connect an Ethernet cable from the laptop to the **MGMT** port on the back of the appliance.
2. Set the IP address of the laptop to 192.168.1.100, the subnet mask to 255.255.255.0, and no default gateway.

Step 6: Log into Safeguard for Privileged Passwords

1. Open a browser on the laptop and connect to the IP address of the **MGMT** port https://192.168.1.105.

If you have problems accessing the configuration interface, check your browser Security Settings or try using an alternate browser.

2. Accept the certificate and continue. This is only safe when using an Ethernet cable connected directly to the appliance.
3. Log into the Safeguard for Privileged Passwords Web client using the bootstrap administrator account:
    - User name: ***admin***
    - Password: ***Admin123***

    IMPORTANT: To keep your Safeguard for Privileged Passwords Appliance secure, change the default password for the bootstrap administrator's account.

    To change the password from the web client, click **Settings** in the upper right corner of the screen and select **Change Password**.
4. Configure the primary network interface (X0):
    a. On the **Appliance Configuration** page, configure the following. Click the **Edit** icon to modify these settings.
        - **Time**: Enable NTP and set the primary NTP server; if desired, set the secondary NTP server, as well. Click **Save**. By default, the NTP server is set to pool.ntp.org.
        - **Network (X0)**:
            - Enter the appliance's IPv4 and/or IPv6 address information (IP address, Subnet Mask, Gateway)
            - Enter the DNS server address.
            - Optional, enter the DNS suffixes.
            - Click **Save**.

    NOTE: The **Network Interface (X1)** information must be configured to use the embedded sessions module. You can configure the **Network Interface (X1)** for the Privileged Sessions module now or later using the Windows desktop client or web client.

    If one or more Safeguard Sessions Appliances are joined to Safeguard for Privileged Passwords, X1 is not available in Safeguard for Privileged Passwords.

Step 7: Connect the appliance to the network

- Connect an Ethernet cable from your primary interface (X0) on the appliance to your network.

Step 8: Configure Safeguard for Privileged Passwords

NOTE: When you install the Windows desktop client, the following is also installed:

- Safeguard for Privileged Passwords PuTTY which is used to launch the SSH client for SSH session requests.

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.

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. Click this link: 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*.

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

1. Log in using the bootstrap administrator account from Step 6: Log into Safeguard for Privileged Passwords.

2. Run the desktop client and log in with the configured IPv4 or IPv6 address for the primary interface (X0). To log in with an IPv6 address, enter it in square brackets.
3. License one or both of the Safeguard for Privileged Passwords modules using the provided license files:
    - Privileged passwords
    - Embedded sessions module
4. Designate an archive server for storing session recordings. Defining archive server configurations and assigning an archive server to an appliance are done from the desktop's **Administrative Tools** view:
    - Go to **Settings** | **Backup and Retention** | **Archive Servers** to configure archive servers.
    - Go to **Settings** | **Sessions** | **Session Recordings Storage Management** to assign an archive server to an appliance for storing recording files.
5. To configure the time zone:
    a. Navigate to **Administrative Tools** | **Settings** | **Safeguard Access** | **Time Zone**.
    b. Select the time zone in the **Default User Time Zone** drop-down menu.
6. Ensure that your Safeguard for Privileged Passwords Appliance has the latest software version installed. To check the version:
    a. From the Safeguard for Privileged Passwords Desktop Client, log in with admin account credentials.
    b. Click **Settings** | **Appliance** | **Appliance Information**. The **Appliance Version** is displayed.
    c. Go to the following product support page for the latest version:

    https://support.oneidentity.com/one-identity-safeguard/download-new-releases
    d. If necessary, apply a patch. Wait for maintenance. If you are installing multiple patches, repeat as needed.

Step 9: Backup Safeguard for Privileged Passwords

Immediately after your initial installation of Safeguard for Privileged Passwords, make a backup of your Safeguard for Privileged Passwords Appliance.

NOTE: The default backup schedule runs at 22:00 MST, which can be modified rather than manually running a backup.

1. From the Safeguard for Privileged Passwords desktop Home page, select **Administrative Tools**.
2. In **Settings**, select **Backup and Retention** | **Backups**.
3. Click **+ Run Now**.

Step 10: Update Safeguard for Privileged Passwords

Download the latest update from: https://support.oneidentity.com/one-identity-safeguard/.

1. From the Safeguard for Privileged Passwords desktop Home page, select **Administrative Tools**.
2. In **Settings**, select **Appliance** | **Updates**.
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. Click **Install Now** to install the update file immediately.
5. Once you have updated Safeguard for Privileged Passwords, be sure to backup your Safeguard for Privileged Passwords Appliance.

Step 11: Add a user with Authorizer administrative permissions

The Authorizer administrator is responsible for granting administrative access to One Identity Safeguard for Privileged Passwords.

1. From the Safeguard for Privileged Passwords desktop Home page, select **Administrative Tools**.

   NOTE: This is where you add all the objects you need to write access request policies, such as users, accounts, and assets.

2. In **Administrative Tools**, select **Users**.
3. Click **+ Add User** to create a Safeguard for Privileged Passwords user with a "local" authentication provider and Authorizer Administrator permissions.

Username	Password	Permissions	Description
AuthorizerAdmin	Test123	Authorizer	The administrator responsible for granting all administrative access to Safeguard for Privileged Passwords.

   NOTE: When you choose **Authorizer** permissions, Safeguard for Privileged Passwords also selects **User** and **Help Desk** permissions. These additional settings cannot be cleared.

4. Log out:
   a. In the upper-right corner of the screen, click the user avatar.
   b. Select **Log Out**.

Step 12: Change the local security policy

Before One Identity Safeguard for Privileged Passwords can reset local account passwords on Windows systems, you must change the local security policy.

1. From the Windows Start menu, open **Local Security Policy**.
2. Navigate to **Local Policies** | **Security Options**.
3. Disable "User Account Control: Run all administrators in Admin Approval Mode" option.
4. Restart your computer.

Step 13: Enable password authentication (applies to Privileged Sessions module only)

For some systems (SUSE and some Debian systems) that use SSH, you must enable password authentication in the package generated configuration file (sshd_config).

For example, in the debian sshd_config file, enable the following parameter: PasswordAuthentication yes

Creating local administrator users

Once you have successfully installed the desktop client application, you must add the objects you need to write access request policies, such as users, accounts, and assets. If your company practices the principles of separation of duties (SoD), the Authorizer Administrator needs to create the following additional administrators.

NOTE: A user can be assigned more than one set of permissions.

To add local administrator users

1. Log into the Windows desktop client application as *AuthorizerAdmin*.
2. From the **Home** page, navigate to **Administrative Tools** and select **Users**.
3. Add the following additional local administrator users:

Username	Password	Permissions	Description
ApplianceAdmin	Test123	Appliance	The administrator responsible for configuring the appliance.
AssetAdmin	Test123	Asset	The administrator responsible for adding and managing partitions, assets, and accounts.

Username	Password	Permissions	Description
Auditor	Test123	Auditor	The administrator responsible for reviewing all access request activity.
PolicyAdmin	Test123	Security Policy	The administrator responsible for defining the entitlements and policies that control which assets and accounts a user can access.
UserAdmin	Test123	User	The administrator responsible for managing users.

NOTE: When you choose certain permissions, Safeguard for Privileged Passwords also selects additional permissions. Do not clear these additional settings.

Before you log out, let's see if Safeguard for Privileged Passwords added these users.

To view the audit log

1. From the **Home** page, navigate to the **Activity Center**.
2. Leave the default search criteria (I would like to see all activity occurring within the last 24 hours).
3. Click **Run**.
4. Explore the results.

   As the Authorizer Administrator, you can view User Authentication and Object History for Audit Events pertaining to users.
5. Log out.

Configuring external integration settings

First we will log into the desktop client with an Appliance Administrator account (*ApplianceAdmin*) to configure the following external integration settings:

- Starling join (used for secondary authentication and Approval Anywhere)
- Email notifications

Setting up a Starling account

We will be using Starling Two-Factor Authentication as our service provider for secondary authentication and Approval Anywhere. To get started, you must register a Starling Organization Admin account or a Collaborator account associated with the One Identity Hybrid subscription. Also, you must download the **Starling 2FA** app on your mobile phone to use the Approval Anywhere feature.

NOTE: For additional information and documentation regarding the Starling Cloud platform and Starling Two-Factor Authentication, see https://support.oneidentity.com/starling-two-factor-authentication/hosted/technical-documents.

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.

Joining Starling

One Identity Starling Two-Factor Authentication is a software-as-a-service solution that provides two-factor authentication on a product enabling 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 and Starling Identity Analytics & Risk Intelligence.

Joining Safeguard for Privileged Passwords to Starling addsSafeguard for Privileged Passwords to the One Identity Hybrid service allowing you to use features from both the Starling Two-Factor Authentication and Starling Identity Analytics & Risk Intelligence services.

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 service 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 in to Safeguard for Privileged Passwords.

- Approval Anywhere

  The Safeguard for Privileged Passwords Approval Anywhere feature integrates its access request workflow with Starling Two-Factor Authentication, 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.

Later in the guide, we will step through the process of configuring a user to require two-factor authentication as well as logging in with two-factor authentication. We will also discuss how to define the users who are authorized to use Approval Anywhere to approve access requests.

To join Safeguard for Privileged Passwords to Starling

1. Log into the Windows desktop client as *ApplianceAdmin*.
2. From the **Home** page, navigate to **Administrative Tools** | **Settings** | **External Integration** | **Starling**.
3. 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**. In addition, the **Administrative Tools** | **Settings** | **External Integration** | **Secondary Authentication** pane displays **Starling 2FA** as a secondary authentication provider.

Stay logged in as the *ApplianceAdmin* for setting up email notifications.

Setting up email notifications

To demonstrate how Safeguard for Privileged Passwords sends out event notifications, you must configure Safeguard for Privileged Passwords to automatically send email notifications when certain events occur. For the purposes of this software evaluation, we have you set up a template for Access Request Auto-Approval.

To setup email notifications

1. Navigate to + **Administrative Tools** and select **Settings**.
2. In **Settings**, select **External Integration** | **Email**.
3. To configure the **Email** notifications, enter these settings for all Safeguard for Privileged Passwords emails:

SMTP Server Address	Enter the IP address or FQDN of the mail server. 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.
Sender Email	Enter your email address.
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 your email address as the **Send To** email address and click **Send**.

   Safeguard for Privileged Passwords sends an email using the configuration settings.

Creating local users

Standard users do not have any Safeguard for Privileged Passwords administrative permissions. These users can be granted rights to request access, approve access requests, or review completed access requests. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Adding a user* section.

NOTE: You can perform the exercises in this guide with directory users as well as local users. To do that, you must add a directory, directory users, and an authentication provider.

To streamline your software evaluation, we recommend that you simply use local users. The access request workflow is the same no matter what users perform them. To make your user experience more realistic, you can set up other local users from your test lab to be a "Requester", "Approver", and "Reviewer" or use the test users we suggest creating below.

To create local users

1. Log into the Windows desktop client as *UserAdmin*.
2. From the **Home** page, navigate to **Administrative Tools** and select **Users**.
3. In **Users**, click **+ Add User** to add the following Safeguard for Privileged Passwords non-administrator users:

Username	Password	Permissions	Description
Joe	Test123	None	The "Requester user", authorized to request access.
Abe	Test123	None	The "Approver user", authorized to approve access requests. See the following procedure for more information on how to configure Abe for two-factor authentication.
Ralph	Test123	None	The "Reviewer user", authorized to review past (or completed) access requests.
Pete	Test123	None	The delegated partition owner.

To configure a user for two-factor authentication

NOTE: Abe will be authorized to approve access requests.

1. As the *UserAdmin* add a new local user named "Abe".
2. On the Authentication page,
    a. **Authentication Provider**: Select **Local**.
    b. **User Name**: Enter **Abe**.
    c. **Password** | **Confirm Password**: Enter **Test123**.
    d. **Require Secondary Authentication**: Select this check box.
    e. **Authentication Provider**: Select the **Starling 2FA** service provider.
    f. **Use alternate mobile phone number**: Optionally, select this check box and enter an alternate mobile number to be used for two-factor authentication notifications.
3. On the Contact page,
    a. **Mobile Phone**: Enter your mobile phone number.
    b. **Email Address**: Enter a valid email address.
4. Finish adding the local user to Safeguard for Privileged Passwords.
5. Log out of Safeguard for Privileged Passwords.
6. Log in as the *PolicyAdmin* and navigate to **Administrative Tools** | **Settings** | **External Integration** | **Approval Anywhere**.
7. Click **+ Add** to add *Abe* as a user authorized to use the Approval Anywhere feature.
8. Log out of Safeguard for Privileged Passwords.

Adding assets and accounts

Now let's add some systems so that you can see how Safeguard for Privileged Passwords manages them. A background in the assets, entities, partitions, and accounts will help your understanding. For more information see the following sections in Overview of the entities :

- Assets, partitions, and partition profiles
- Accounts, account groups, entitlements, and entitlement access request policies

To add partitions, assets, and accounts to Safeguard for Privileged Passwords

1. Log in as *AssetAdmin* and navigate to **Administrative Tools**.
2. In **Partitions**, click **+ Add Partition** to add these partitions. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Adding a partition* section.

Partition	Description	Delegated Owner
Linux Servers	The Linux Administrator's workspace.	Pete
Windows Servers	The Windows Administrator's workspace.	none
Directory	The Directory Administrator's workspace.	none

3. Configure the **Profile** check and change schedules to run daily. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Creating a partition profile* section.
    a. Navigate to **Settings** | **Profile** | **Check Password** (and **Change Password**).
    b. Double-click each schedule to modify the schedule.
    c. Select **Schedule** and choose the **Day** interval, set the time of day, and leave the daily repeat interval set to 1 day.
4. In **Assets**, add some Linux, Windows, and Directory devices. Be sure to put them into the appropriate partition. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Adding an asset* section.

    NOTE: To observe how Safeguard for Privileged Passwords automatically changes passwords, setup assets from your test lab, with actual network addresses, service accounts, and passwords.

    Run **Test Connection** on the **Connection** tab to ensure that Safeguard for Privileged Passwords can communicate with the asset.

    a. Once you add an asset, add one or more unique accounts for each asset. These are the accounts Safeguard for Privileged Passwords will use to give people access to the asset. In **Assets**, select the asset and opened the Accounts tab. Click + **Add Account**. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Adding an account to an asset* section.
    b. After you add the account, right-click (or press and hold) the new account to set the password (**Account Security** | **Set Password**).
    c. Make the asset available for discovery. Select the asset then, on the **General** pane, scroll to **Account Discovery** and click **Edit**. Add the details for the discovery including the rules.
5. Log out.

Writing entitlements

Now that we have demonstrated that Safeguard for Privileged Passwords is actually managing your account passwords, let's define some rules for requesting password release and session access requests, such as the maximum duration, how many approvals are required, and so forth.

For more information see the following section in Overview of the entities

To write the entitlements that govern access requests

1. Log in as *PolicyAdmin* and navigate to **Administrative Tools**.
2. In **Settings**, select **Access Request** | **Reasons** and add these access request reason codes:

Reason	Description
SU	Software Updates
Sys Maint	System Maintenance
SSH Session	SSH Session Request
RDP Session	RDP Session Request

3. In **User Groups** add these user groups. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Adding a user group* section.

User Groups	Description	User
Approvers	Users authorized to approve password release requests.	Abe
Requesters	Users authorized to request passwords.	Joe
Reviewers	Users authorized to review password release requests.	Ralph

   a. On the **Users** tab, add each user to the specified user group.

4. In **Account Groups**, add the following account groups. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Adding an account group* section.

Account Group	Description
Linux Server Accounts	Accounts for the Linux machines

Account Group	Description
Windows Server Accounts	Accounts for the Windows machines.
Directory Server Accounts	Accounts for the Directory machines.

   a. On the **Accounts** tab, add the appropriate accounts to each account group.

5. In **Entitlements**, add the following entitlements. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Adding an entitlement* section.

   NOTE: At this time, do not set entitlement time restrictions.

Entitlement	Description
Linux Password Requests	The rules that govern password release requests for the Linux Servers.
Windows Password Requests	The rules that govern password release requests for the Windows Servers.
Directory Password Requests	The rules that govern password release requests for the Directory Servers.
Sessions Requests	The rules that govern session access requests.

6. Stay logged in as the Security Policy Administrator (*PolicyAdmin*) and proceed to the next exercise.

Now let's add access request policies to each of these entitlements that restrict system access to authorized users.

Adding password release request policies

We now need to define the users who are authorized to make password release requests and add access request policies to define the scope (accounts that can be accessed) and rules for checking out passwords. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Creating an access request policy* section.

To add a policy to the Linux Password Requests Entitlement

1. As *PolicyAdmin* navigate to **Administrative Tools** | **Entitlements** .
2. Select the **Linux Password Requests Entitlement**.
3. On the **Users** tab, add the *Requesters* user group as the "user" for this entitlement.

   An entitlement "User" is a person who is authorized to request passwords to accounts governed by the polices in the entitlement.

4. On the **Access Request Policies** tab, create the following access request policy:
    a. **General** tab:
        - Policy Name: *Linux Servers Password Release Request Policy*
        - Description: *The rules that define the request, approval, and review of password release requests for the Linux Server Accounts.*
        - Access Type: **Password Release**.
    b. **Scope** tab:
        - *Linux Server Accounts* group
    c. **Requester** tab:
        - Select the following reasons: **SU** and **Sys Maint**.
        - Require a **Reason**.
        - Require a **Comment**.
        - Select the **Allow Requester to Change Duration** option.
    d. **Approver** tab:
        - Require one person from the *Approvers* user group to approve a password release request.
    e. **Reviewer** tab:
        - Require one person from the *Reviewers* user group to review a completed password release.
    f. **Access Config** tab
        - Select the **Change password after check-in** option.
    g. **Time Restrictions** tab:
        - Do not set policy Time Restrictions.
    h. **Emergency** tab:
        - Enable Emergency Access.

To add a policy to the Windows Password Requests Entitlement

1. As *PolicyAdmin* navigate to **Administrative Tools** | **Entitlements**.
2. Select the **Windows Password Requests Entitlement**.
3. On the **Users** tab, add the *Requesters* user group as the "user" for this entitlement.

   An entitlement "User" is a person who is authorized to request passwords to accounts governed by the polices in the entitlement.
4. On the **Access Request Policies** tab, create the following access request policy:
    a. **General** tab:
        - Policy Name: *Weekday Maintenance Policy*

- Description: *The rules that define the request, approval, and review of password release requests for the Windows Server Accounts on weekdays.*
- Access Type: **Password Release**

b. **Scope** tab:

- *Windows Server Accounts* group

c. **Requester** tab:

- Do not require a Reason.
- Do not require a Comment.
- Select the **Allow Requester to Change Duration** option.

d. **Approver** tab:

- Require one person from the *Approvers* user group to approve a password release request.

e. **Reviewer** tab:

- Require one person from the *Reviewers* user group to review a completed password release.

f. **Access Config** tab

- Select the **Change password after check-in** option.

g. **Time Restrictions** tab:

- Allow users to access passwords in the scope of this policy anytime Monday through Friday.

h. **Emergency** tab:

- Do not Enable Emergency Access.

To add a policy to the Directory Requests Entitlement

1. As *PolicyAdmin* navigate to **Administrative Tools** | **Entitlements**.
2. Select the **Directory Password Requests Entitlement**.
3. On the **Users** tab, add the *Requesters* user group as the "user" for this entitlement.

   An entitlement "User" is a person who is authorized to request passwords to accounts governed by the polices in the entitlement.
4. On the **Access Request Policies** tab, create the following access request policy:

   a. **General** tab:

   - Policy Name: *Weekday Maintenance Policy*
   - Description: *The rules that define the request, approval, and review of password release requests for the Windows Server Accounts on weekdays.*
   - Access Type: **Password Release**

   b. **Scope** tab:

- *Directory Server Accounts* group

c. **Requester** tab:
   - Do not require a Reason.
   - Do not require a Comment.
   - Select the **Allow Requester to Change Duration** option.

d. **Approver** tab:
   - Require one person from the *Approvers* user group to approve a password release request.

e. **Reviewer** tab:
   - Require one person from the *Reviewers* user group to review a completed password release.

f. **Access Config** tab
   - Select the **Change password after check-in** option.

g. **Time Restrictions** tab:
   - Allow users to access passwords in the scope of this policy anytime Monday through Friday.

h. **Emergency** tab:
   - Do not Enable Emergency Access.

Adding session request policies

Prior to requesting a session, you must create a session request policy that defines the users who are authorized to access an asset or account. As part of this request policy you will also define the protocol (SSH or RDP) to be used as well as the type of account credentials to be specified to access the asset or account.

To write the policies that govern session requests

1. As *PolicyAdmin* navigate to **Administrative Tools** | **Entitlements**.
2. Select the **Sessions Requests** entitlement.
3. On the **Users** tab, add the *Requesters* user group as the "user".
4. On the **Access Request Policies** tab, create the following access request policies for the sessions request entitlement:
   a. Create a policy for SSH sessions:

      General tab:
      - Policy Name: *SSH Session Request Policy*
      - Description: *The rules that define the request, approval, and review of*

session requests using SSH protocol.

- Access Type: **SSH**

Scope tab:

- *Linux Server Accounts* group

Requester tab:

- Select the following reason: **SSH Session**.
- Require a Reason.
- Require a Comment.
- Select the **Allow Requester to Change Duration** option.

Approver tab:

- Require one person from the *Approvers* user group to approve a session request.

Reviewer tab:

- Require one person from the *Reviewers* user group to review a session release.

Access Config tab

- Use the default settings (**None** is selected by default).

Session Settings tab

- Select **Record Sessions**.
- Select **Enable Command Detection**.
- Leave the **SSH Controls** selected:
  - **Allow SFTP**
  - **Allow SCP**
  - **Allow X11 Forwarding**

Time Restrictions tab:

- Do not set policy time restrictions.

Emergency tab:

- Do not enable emergency access.

b. Create a policy for RDP sessions:

General tab:

- Policy Name: *RDP Session Request Policy*
- Description: *The rules that define the request, approval, and review of session requests using RDP protocol.*
- Access Type: **RDP**

Scope tab:

- *Windows Server Accounts* group.

Requester tab:

- Do not select or require a reason.
- Do not require a comment.
- Select the **Allow Requester to Change Duration** option.

Approver tab:

- Select **Auto-approved**.
- Click the **To** button to **Notify when Account is Auto-Approved** and select the Safeguard for Privileged Passwords user to receive the email notification.

Reviewer tab:

- Require one person from the *Reviewers* user group to review a past session release.

Access Config tab:

- Select **User Supplied**.

Session Settings tab:

- Select **Record Sessions**.
- Leave the **RDP In-Session Controls** selected:
  - Allow **Clipboard**

Time Restrictions tab:

- Do not set policy time restrictions.

Emergency tab:

- Do not enable emergency access.

5. Log out.

3

Password release workflow exercises

Now that you have setup One Identity Safeguard for Privileged Passwords, it's time to validate the access request policies you created for password release requests.

Exercise 1: Testing the password release workflow

This exercise demonstrates the password release workflow from request to approval to review.

NOTE: If you setup users from your test lab as a "Requester", "Approver", and "Reviewer" user, have each of them log into a web client using a mobile device. If mobile devices are not available, have your users log into the Safeguard for Privileged Passwords desktop client at their own workstations.

To start the Web application

1. Open a browser and navigate to: **HTTPS://<*Appliance IP Address*>**
2. Start three instances of the web client, logging in as *Joe*, *Abe*, and *Ralph*, respectively.

   NOTE: Alternatively, you can open three browser windows on a single desktop and display them side-by-side to simulate mobile devices. Log into each instance as your "Requester", "Approver", and "Reviewer" users.

Test: Request password

1. As *Joe*, the "Requester" user.
2. On your **Home** page, select **New Request**.
    - If you have set up a Linux account and a Windows account, request a password from each.
3. Use the default access options.
    - Notice how the policy configuration changes the user experience.
4. Open **Requests** and review your pending requests.

Test: Approve password requests

NOTE: Did you receive a notification on your mobile phone? You can approve the request from your mobile device without being logged into Safeguard for Privileged Passwords.

If you'd rather approve it using the desktop client proceed to the steps below.

1. As *Abe*, the "Approver" user.

    NOTE: Notice Abe has an additional authentication step to take in order to log into Safeguard for Privileged Passwords. In addition, since we have set up Approval Anywhere you can use the Starling 2FA app on your mobile phone to complete the login process.

2. Open **Approvals** and review the requests waiting for your approval.
3. Select **Approve/Deny** to approve *Joe*'s password requests.

Test: The password and check it in

1. As *Joe*.
2. Once the password becomes **Available**, open the requests and select **Show Password** to see the password on your screen.
    - Make note of the password so that you can verify that Safeguard for Privileged Passwords changes it after you use it.
3. Select **Copy**.
4. Using the password in your copy buffer, log into the test server.
5. Log out of the test server and return to the Safeguard for Privileged Passwords desktop.
6. Select **Check-In** to complete the password checkout process for the password requests.

Test: Review a password release

1. As *Ralph*, the "Reviewer" user.
2. Open **Reviews** and review the requests that are waiting for your review.
    a. Select **Workflow** to view the transactions that took place as part of the request.
    b. Select **Review** to enter a comment and complete the review process.

Test: Request emergency access

1. As *Joe*.
2. Request the password for the Linux asset again, this time use the **Emergency Access** option.
    - Notice that the password becomes immediately available. That is because **Emergency access** bypasses the approval.
3. Once the password becomes **Available**, open the password request and select **Show Password**.
    - Is the password different this time? When the **Change Password After Release** option is selected in the policy, Safeguard for Privileged Passwords automatically changes the password after each use.
4. **Copy** the password so you can use it to manually log into the remote asset/account.
5. After you have successfully logged into the remote asset/account, log out of the test server and return to the Safeguard for Privileged Passwords desktop.
6. Select **Check-In**.

Test: Review a password release

1. As *Ralph*.
2. Open **Reviews** and review the requests that are waiting for your review.
3. a. Select **Workflow** to view the transactions that took place as part of the request.
    b. Select **Review** to enter a comment and complete the review process.

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 (*PolicyAdmin*) 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.

Exercise 2: Testing time restrictions

Now that you have seen the end-to-end password release process from request to approval to review, let's demonstrate how the entitlement and policy time restrictions affect a

password request.

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.

Test: Entitlement time restrictions

1. As PolicyAdmin, navigate to **Entitlements**.
2. Navigate to the **General** tab of the *Linux Password Requests* entitlement.
3. Set the entitlement **Time Restrictions** to allow users to access passwords only during their lunch hour Monday through Friday.
4. As *Joe*, assuming that it is currently *not* during your lunch hour, request a password for a Linux account, for a duration of 5 minutes.
    - Did Safeguard for Privileged Passwords allow you to check out this password? The request dialog disables the **Request Immediately** option. The request time will automatically be set for the next unrestricted time frame that allows the account password to be requested.
5. **Cancel** the request (or return to your *Home* page).

Test: Entitlement expiration

1. As PolicyAdmin, set the **Time Restrictions** for the *Linux Password Requests* role to 8:00 a.m. - 5:00 p.m. Monday through Friday.
2. While you are in **Time Restrictions**, set this entitlement to expire today in 1 minute from now.
3. Wait for the entitlement to expire.
    - Did you see Safeguard for Privileged Passwords's notification?

      NOTE: If you do not see the notification refresh your screen.
4. As *Joe*, request a password for a Linux account.
    - Notice that the account is not available to check out. Safeguard for Privileged Passwords does not allow you to checkout accounts associated with expired entitlements.
5. As PolicyAdmin, remove the expiration time from the **Time Restrictions**, but leave the entitlement Time Restrictions enforced.

6. As *Joe*, request a password for the same Linux account.
    - Observe that you are now allowed to request passwords for the *Linux Password Requests* accounts.
7. **Cancel** the request (or return to your Home page).

Test: Policy time restrictions

1. As PolicyAdmin, set the policy **Time Restrictions** for the *Weekday Maintenance Policy* to allow users to access passwords 8:00 a.m. - 5:00 p.m. Monday through Friday.
2. As *Joe*, request a password for the Windows account for Sunday at 2:00 p.m.
    - This request was denied because the *Weekday Maintenance Policy* does not allow you to check out accounts on Sunday.
3. **Cancel** the request (or return to your Home page).

Exercise 3: Testing priorities

To determine which policy to use for a password release, Safeguard for Privileged Passwords considers both entitlement and policy priorities. Safeguard for Privileged Passwords first considers the entitlement priority, then the priorities of policies within that entitlement.

Test: Entitlement priorities

To test entitlement priorities, an account must be governed by two different entitlements.

1. As PolicyAdmin, navigate to **Entitlements**.
2. Verify that the *Linux Password Requests* entitlement is priority #1.

    NOTE: Safeguard for Privileged Passwords displays the priority number under the entitlement name.

3. In **Account Groups**, add the Windows account to the *Linux Servers Accounts* group.
4. As *Joe*, request a password for the Windows account, for Sunday at 9:00 a.m.
    - Are **Reasons** and a **Comment** required? If so, then you know that Safeguard for Privileged Passwords used the *Linux Password Requests* entitlement; the *Windows Password Requests* entitlement does not require **Reasons** or **Comments**.
    - Did the **Time Restriction** prevent you from checking out this password? The *Linux Password Requests* entitlement only allows you to checkout passwords Monday through Friday, from 8:00 a.m. to 5:00 p.m.
5. **Cancel** the request.

6. As PolicyAdmin, change the priority of these entitlements, making the *Windows Password Requests* priority #1, and run through this test again to see if you get different results.
    - Are **Reasons** and a **Comment** required? If not, then you know that Safeguard for Privileged Passwords used the *Windows Password Requests* entitlement as it does not require **Reasons** or **Comments**.
    - Did the **Time Restriction** prevent you from checking out this password? The *Weekday Maintenance Policy* only allows you to checkout passwords Monday through Friday, from 8:00 a.m. to 5:00 p.m.
7. Before you leave this test, change the priority back and remove the Windows account from the *Linux Servers Accounts* group.

Test: Policy priorities

To test policy priorities, an account must be in the scope of two policies within the same entitlement.

1. Log in as PolicyAdmin and navigate to **Administrative Tools**.
2. In **Entitlements**, add this new policy to the *Windows Password Requests* entitlement:

    General tab:
    - Policy Name: *Sunday Maintenance Policy*.
    - Description: *The rules that define the request, approval, and review of password requests for the Windows Server Accounts on Sundays.*
    - Access Type: **Password Release**

    Scope tab:
    - *Windows Server Accounts* group

    Requester tab:
    - Select all Reasons.
    - Require a Reason.
    - Require a Comment.
    - Select the **Allow Requester to Change Duration** option.

    Approver tab:
    - Require one person to approve a password request, then select the *Abe* account.

    Reviewer tab:
    - Require one person to review a past password release, then select the *Ralph* account.

    Access Config tab:

- Ensure access type is **Password Release**
- Select the **Change password after Check-in** check box.

Time Restrictions tab:

- Allow users to checkout passwords only on Sunday.

Emergency tab:

- Enable Emergency Access.

3. Verify that the *Weekday Maintenance Policy* is priority #1.
4. As *Joe*, request a password for the Windows account, for Sunday at 9:00 a.m.
   - Are you required to add a **Reason** for your password request?

     If not, then you know Safeguard for Privileged Passwords used the *Weekday Maintenance Policy* which does not have **Reasons** or **Comments** enabled.
   - Did the **Time Restrictions** prevent you from checking out this password?

     The *Weekday Maintenance Policy* does not permit you to request a password on Sunday.
5. **Cancel** the request.
6. As PolicyAdmin, change the priority of these policies, making the *Sunday Maintenance Policy* priority #1, and run through this test again to see if you get different results.
   - Are you required to add a **Reason** for your password request?

     If so, then you know Safeguard for Privileged Passwords used the *Sunday Maintenance Policy*; the *Weekday Maintenance Policy* does not have **Reasons** or **Comments** enabled.
   - Did the **Time Restrictions** prevent you from checking out this password?

     The *Sunday Maintenance Policy* permits you to request a password on Sunday.
7. Before you leave this test, change the policy priority back.
8. Cancel the request and log out.

Sessions access request exercises

The embedded sessions module in One Identity Safeguard for Privileged Passwords enables you to issue privileged access to users for a specific period or session and gives you the ability to record, archive, and replay user sessions so that your company can meet its auditing and compliance requirements.

CAUTION:The embedded sessions module in Safeguard for Privileged Passwords version 2.7 will be removed in a future release (to be determined). For uninterrupted service, organizations are advised to join to the more robust Safeguard for Privileged Sessions Appliance for sessions recording and playback.

Before you begin:

- Appliance Administrator: Ensure the embedded sessions module for Safeguard for Privileged Passwords is licensed (**Settings** | **Appliance** | **Licensing**).
- Appliance Administrator: Ensure the Network Interface X1 is configured (**Settings** | **Appliance** | **Networking**).
- Appliance Administrator: Ensure the session request service is enabled (**Settings** | **Access Request** | **Enable or Disable Services**).
- Appliance Administrator: Safeguard for Privileged Passwords ships with default session certificates; however, it is recommended that you replace the default certificate with your own (**Settings** | **Certificates** | **Session Certificates**).
- Security Policy Administrator: Ensure there is an entitlement with an access request policy for both SSH and RDP sessions defined. For more information, see Writing entitlements on page 47.
- Ensure Remote Desktop is enabled for Windows machines that are going to be using RDP.
- Ensure the necessary SSH algorithms are configured for any Unix or Linux machines that are going to be using SSH.

  NOTE: Safeguard for Privileged Passwords ships with default SSH algorithms configured for Unix and Linux machines. To add new algorithms, use the API endpoint:

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

These exercises will guide you through a step-by-step evaluation of the Safeguard for Privileged Passwords session request workflow process:

Exercise 1: Testing the SSH session request workflow

This exercise demonstrates the SSH session request workflow from request to approval to review.

Test: Request session

1. As *Joe*, the "Requester" user.
2. On your **Home** page, select **New Request**.
   - Request an SSH session for a Linux account.
   - Notice how the policy configuration dictates the user experience. For example, you are required to enter a reason and a comment.
3. Open **Requests** and review your pending request.

Test: Approve sessions request

NOTE: Did you receive a notification on your mobile phone? You can approve the request from your mobile device without being logged into Safeguard for Privileged Passwords.

If you'd rather approve it using the desktop client proceed to the steps below.

1. As *Abe*, the "Approver" user.

   NOTE: Notice Abe has an additional authentication step to take in order to log into Safeguard for Privileged Passwords. In addition, since we have set up Approval Anywhere you can use the Starling 2FA app on your mobile phone to complete the login process.

2. Open **Approvals** and review the request waiting for your approval.
3. Select **Approve/Deny** to approve *Joe*'s session request.

Test: Launch the SSH session

1. As *Joe*.
2. Once the session becomes **Available**, open the session request and select ▶

Launch SSH client.

The **PuTTy Configuration** dialog displays pre-populated with the required information, click **Open**.

3. Accept the security certificate to continue.
4. Perform various commands on the test server.
5. Log out of the test server and return to the Safeguard for Privileged Passwords desktop.
6. Select **Check-In** to complete the checkout process for the sessions request.

Test: Review a completed sessions request

1. As *Ralph*, the "Reviewer" user.
2. Open **Reviews** and review the request that is waiting for your review.
3. Select **Workflow** to view the transactions that took place as part of the request.
    a. Since **Record Sessions** is enabled in the policy, on the Initialize Session event, click **Play** to replay the session.
    b. Since **Enable Command Detection** is enabled in the policy, on the Initialize Session event, click the **events** link to view a list of the commands and programs run during the session.
4. Select **Review** to complete the review process.

Exercise 2: Testing the RDP session request workflow

This exercise demonstrates the RDP session request workflow from request to approval to review. Since the entitlement's policy specified that you will provide your own credentials, you will need to enter those before you launch the RDP session.

Test: Request session

1. As *Joe*, the "Requester" user.
2. On your **Home** page, select **New Request**.
    - Request an RDP session for a Windows account.
    - Notice how the policy configuration dictates the user experience. For example, you are not required to enter a reason and a comment for this policy.
3. Open **Requests** and review your pending request.

Test: Approve sessions request

Since the access request policy was set to **Auto-approved**, there is no approval required.

Did you get an email notification of the auto-approved access request?

Test: Launch the RDP session

1. As *Joe*.
2. Once the session becomes **Available**, open the session request.
3. Enter the credentials to be used (user name and password) and click **Apply**.

   Clicking **Apply** retrieves the information required to log in: Computer ID and Username Connection String.
4. Select **Launch RDP**.
5. Accept the security certificate to continue.
6. Run programs (for example, launch a browser and browse the internet) on the test server.
7. Log out of the test server and return to the Safeguard for Privileged Passwords desktop.
8. Select **Check-In** to complete the checkout process for the sessions request.

Test: Review a completed sessions request

1. As *Ralph*, the "Reviewer" user.
2. Open **Reviews** and review the request that is waiting for your review.
3. Select **Workflow** to view the transactions that took place as part of the request.
   a. Since **Record Sessions** is enabled in the policy, on the Initialize Session event, click **Play** to replay the session.
   b. Notice that since **Enable Window Title Detection** is not enabled in the policy, a list of the windows opened on the desktop during the session are not available for review.
4. Select **Review** to complete the review process.

5

Auditing exercises

Now that you have performed some password request activities, you can audit the transaction data.

The appliance records all activities performed within One Identity Safeguard for Privileged Passwords. Any administrator has access to the audit log information; however, your administrator permission set determines what audit data you can access.

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.
- Check and Change Log: Where you view an account's password validation and reset history.
- History: Where you view the details of each operation that has affected the selected item.
- Activity Center: Where you can search for and review any activity for a specific time frame.
- 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.
- Reports: Where you can view and export entitlement reports that show you which assets and accounts a selected user is authorized to access.

The exercises in this section demonstrate Safeguard for Privileged Passwords's auditing capabilities. But before we start, let's create some password check and change activity.

These exercises will guide you through a step-by-step evaluation of the Safeguard for Privileged Passwords auditing features.

Exercise 1: Creating audit data

By following these steps, you will add some password check and change history to Safeguard for Privileged Passwords's audit log and you will learn how to manually verify and reset account passwords.

To perform password check and change activity

1. Log in as AssetAdmin and navigate to **Administrative Tools**.
2. In **Accounts**, select an account.
3. Open the **Account Security** menu and notice the options: **Check Password**, **Change Password**, and **Set Password** using the **Manual Password** option.

   NOTE: These same options are available from an account's context menu.

4. **Check** the password for the account.

   NOTE: The **Tasks** pane opens when you start a task. You can re-size your desktop client console so that the **Tasks** pane is not covering the **Administrative Tools**.

   The "Check" option verifies the account password is synchronized with the Safeguard for Privileged Passwords database; this action should succeed.

   TIP: If **Check Password** fails, run **Check Asset** from the context menu of the asset to ensure that Safeguard for Privileged Passwords can communicate with it. Then retry the **Check Password** option on the account.

5. Set the password for the account to "*Mypass01*" using the **Manual Password** option.

   The "Manual Password" option manually sets the account password in the Safeguard for Privileged Passwords database; not on the appliance; so now they are not in sync.

6. **Check** the password for the account.

   The "Check" option should fail because the account password is not in sync with the Safeguard for Privileged Passwords database.

7. **Change** the password for the account.

   The "Change" option creates a new account password and synchronizes it on the Safeguard for Privileged Passwords database.

8. **Check** the password for the account again.

   This task should now be successful.

Stay logged in as the *AssetAdmin* for the next exercise.

Exercise 2: Accessing the Password Archive

Password Archive allows you to access a previous password for an account for a specific date.

NOTE: 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.

To access an account's previous password

1. In **Accounts**, select the account you have been working with.
2. Click **Password Archive** from the toolbar.
3. In the **Password Archive** dialog, select today's (or a previous) date.

   TIP: If 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 for the specified date.
5. Either **Copy** the password, or click **OK** to close the dialog.
6. **Close** Password Archive to return to **Accounts**.

Stay logged in as the *AssetAdmin* for the next exercise.

Exercise 3: Viewing the Check and Change log

Each account has a **Check and Change Log** tab that allows you to view an account's password validation and reset history.

To view an account's change history

1. In **Accounts**, select the account you have been working with.
2. Select the **Check and Change Log** tab to view the password change history.
3. Explore the results. Sort the items by **Status** or **Time**.

Stay logged in as the *AssetAdmin* for the next exercise.

Exercise 4: Viewing the History tab

Each of the **Administrative Tools** views has a **History** tab that allows you to view or export the details of each operation that has affected a selected item.

To view the transaction history of an account

1. In **Assets**, select a managed system.
2. Select the **History** tab to view the transaction history.
3. Poke around and notice that each of the **Administrative Tools** (Account, Assets, Partitions, Users, etc.) has a **History** tab.
4. Log out.

Exercise 5: Using the Activity Center

The **Activity Center** is the place to go for troubleshooting issues. The appliance records all activities performed within One Identity Safeguard for Privileged Passwords. Any administrator has access to the audit log information; however, your administrator permission set determines what audit data you can access.

To run an activity report

1. Log in as the Auditor.

   NOTE: The Auditor has read-only access to all features.

2. From the **Home** page, navigate to the **Activity Center**.
3. Use the default query settings: I would like to see *all activity* occurring within the *last 24 hours*.
4. Click **Run**.
5. Explore the results.
6. Double-click an event to see more details; Double-click to close the details.

To filter the content

1. Open the **User** filter list and select AssetAdmin.
2. Sort the records so the latest time is listed first.
3. Double-click a password event to view the details of the event.

Stay logged in as the Auditor for the next exercise.

Exercise 6: Auditing access requests

The **Request Workflow** dialog allows you to audit the transactions that took place within a password release or session request. This dialog can be accessed using the **Workflow** button in the Activity Center view when an access request event is selected in an activity audit log report.

The **Workflow** button also appears to reviewers for completed access requests.

To view the request workflow for a password release or session request

1. Log in as the Auditor.
2. From the **Home** page, navigate to the **Activity Center**.
3. Run an activity audit log report.
4. On the results page, select an access request event and click **Workflow**.

   The **Request Workflow** dialog displays the workflow transactions from request to approval to review.
5. Select **Show Details** to view more information about the request, approval, and review transactions of that request.

Stay logged in as the Auditor for the next exercise.

Exercise 7: Running entitlement 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.

Entitlement reports

One Identity 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.

To run an entitlement report

1. As Auditor, select **Reports** from the Safeguard for Privileged Passwords desktop Home page.

2. Choose to view entitlements by **Asset**.
3. **Browse** to select all assets and click **OK**.
4. In the top pane of the results screen select an asset to see the details.
5. View both the **Total Accounts** tab and the **People** tab.
6. Select an item from the results to drill down into the details about the users and the accounts.
7. Click **Export** to create a file of the search results in a location of your choice.
8. Log out.

Discovery exercises

These exercises will guide you through a step-by-step evaluation of the Safeguard for Privileged Passwords discovery features:

Exercise 1: Discovering assets

Safeguard for Privileged Passwords allows you to set up Asset Discovery jobs to run automatically against the directory assets you have added to Safeguard for Privileged Passwords. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, *Asset Discovery* section.

To create an Asset Discovery job using the Directory Method

1. Log in as the Asset Administrator and navigate to **Administrative Tools** | **Discovery** | **Asset Discovery** tile.
2. Click **+ Add** to create an Asset Discovery job.
3. Provide information for the Asset Discovery job on the following tabs:

Tab	Description
General tab	a. Enter a name for the Asset Discovery job. b. For **Partition**, browse to select the partition. c. For **Method**, select **Directory**.
Information tab	In **Directory**, select the directory.
Rules tab	Click **+ Add** to create an Asset Discovery rule: a. Enter a **Name** for the rule.

Tab	Description
	b. For the **Settings**, click **Add Condition** to define criteria, including the search scope in the directory, then click **OK**. c. On the Asset Discovery Rule dialog, for **Connection Template**, leave the default of **None**. d. For **Asset Profile**, use the default partition profile to govern the discovered assets. e. Keep the **Manged Network** default value and click **OK**.
Schedule tab	You can skip adding the schedule to run the Asset Discovery job since we will run the discovery job manually for this exercise.
Summary tab	Review the discovery job and click **Add Discovery**.

4. In the **Asset Discovery** dialog, select the job and click ▶ **Run Now**. The **Tasks** pop-up shows the progress of the Asset Discovery job.
5. When the **Tasks** pop-up indicates that the job is successful (**Success**), click the **Asset Discovery Results** tile.
6. In the **Asset Discovery Results** grid:
   a. Select **Last 24 Hours**.
   b. Click **Refresh** to show the latest data.
   c. Double-click an Asset Discovery job to see the result of the discovery.
   d. Click on the number of **# Assets Found** to view individual discovered assets.
7. To control management of an asset:
   a. Navigate to **Administrative Tools** | **Assets**.
   b. Right-click the asset then click **Access Requests**.
   c. Choose **Enable Session Request** or **Disable Session Request**.

   NOTE: When you ignore an asset, Safeguard for Privileged Passwords disables it and disables/hides all associated accounts. If you choose to **Enable Session Request** the asset later, Safeguard for Privileged Passwords re-enables all the associated accounts.
8. You can also search the Activity Center for information about discovery jobs that have run. This is the same information as presented in the the **Asset Discovery Results** grid.

a. Click **Home**.

b. Under **I would like to see**, click **Edit** and select **Asset Discovery Activity**.

c. Under **... occurring within the ...**, click **Edit** and select **Last 24 Hours**.

d. Keep the default of **All Activity** in the **Last 24 Hours**.

e. Click the **Run** button.

f. In the results grid, double-click the job to more information then click **Details** to show the progress of the Asset Discovery job.

g. The "Asset Discovery" events are listed in the **Activity Category** column.

9. To view all activity in the last 24 hours, return to the **Activity Center** dialog.

a. Under **I would like to see**, click **Edit** and select **All Activity**.

b. Click the **Run** button.

c. In the grid, **User** column, click the **filter**, and select your **User** name.

d. To display additional columns, click **Column** in the upper right corner and select additional columns, such as **Appliance**, **Asset**, **Object Name**, and **Object Type**.

e. Double-click any of the rows to view additional information.

Set asset connection authentication credentials to define a service account

When **None** is selected as the **Authentication Type**, the discovered assets will not have a service account. In the next steps you will change the **Authentication Type**.

These steps provide valid information only if:

- You have created a directory asset and directory accounts that will be used as the service account for the Windows asset discovered.
- You have Linux assets that are discovered that have QAS installed and are joined to the directory.

1. In **Assets**, select one of the newly discovered assets.
2. On the **General** tab, double-click the **Connection** information box or click the **Edit** icon next to it.
3. Choose an **Authentication Type** of **Directory Account** and provide the service account credentials.

NOTE: Safeguard for Privileged Passwords uses a *service account* to connect to an asset to securely manage passwords for the accounts on that asset.

Exercise 2: Discovering accounts

Safeguard for Privileged Passwords allows you to set up Account Discovery jobs to run automatically against the assets it manages in the scope of a partition.

To create an Account Discovery job

1. Log in as the Asset Administrator and navigate to **Administrative Tools** | **Discovery** | **Account Discovery** tile.
2. Click **Add** to create a new Account Discovery job.
    a. **Browse** to select a partition.
    b. Enter a **Name** for the setting, such as "Daily". **Description** is optional.
    c. Select the **Discovery Type** which is 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. If the **Discovery Type** is **Directory**, select the directory on which the Account Discovery job runs.
    d. **Schedule** the discovery job to run daily starting in about 5 minutes.
    e. In **Rules**, click **Add** to add a rule. Enter a **Name**, select **Find All** in **Find By**, and click **OK**.

    NOTE: If you opt to experiment with finding accounts based on rules, note that all search terms return exact matches and are case sensitive.
3. Click **OK** to save the Account Discovery job.
4. Wait for the Account Discovery job to run.
5. After the Account Discovery job runs see the job results and the accounts discovered. At any time, click **Refresh** to update the information.
    a. Click the **Account Discovery Results** tile to see the results of the discovery job run.
    b. Click the **Discovery Accounts** tile to see the accounts that were discovered.
6. You can also search the **Activity Center** for information about discovery jobs that have run. This is similar information as presented in the the **Account Discovery Results** grid.
    a. Under **I would like to see**, click **Edit** and select **Password Management Activity**.
    b. Click the **Run** button.
    c. In the **Events** column, the **Account Discovery** events display.

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 or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

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

F

H

I

J

L

O

P

R

S

T

W