Safeguard for Privileged Passwords 6.0.9 LTS

Evaluation Guide

Safeguard for Privileged Passwords Evaluation Guide
Updated - 23 February 2021, 09:53
Version - 6.0.9 LTS

Contents

1

Introduction

The *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 proof of concept (POC) of its capabilities in your own test lab

Introduction to Safeguard for Privileged Passwords

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

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

Safeguard privileged management software suite

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

The Safeguard products' unique strengths are:

- One-stop solution for all privileged access management needs
- Easy to deploy and integrate
- Unparalleled depth of recording

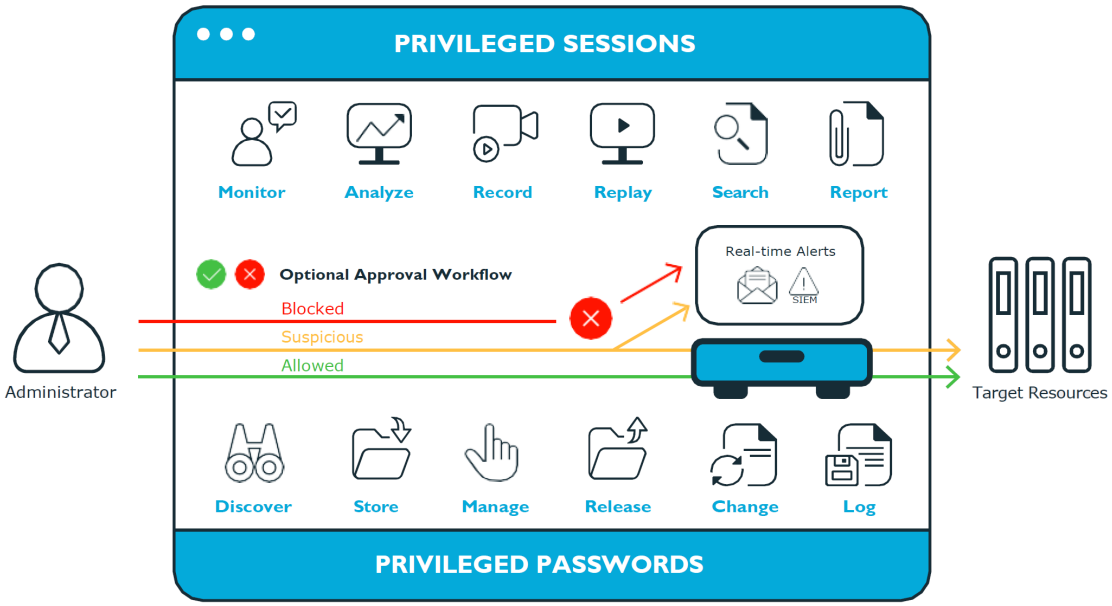
- Comprehensive risk analysis of entitlements and activities
- Thorough Governance for privileged account

The suite includes the following modules:

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

  Safeguard for Privileged Sessions is a quickly deployable enterprise appliance, completely independent from clients and servers to integrate seamlessly into existing networks. It captures the activity data necessary for user profiling and enables full user session drill-down for forensics investigations.
- **One Identity Safeguard for Privileged Analytics** integrates data from Safeguard for Privileged Sessions to use as the basis of privileged user behavior analysis. Safeguard for Privileged Analytics uses machine learning algorithms to scrutinize behavioral characteristics, and generates user behavior profiles for each individual privileged user. Safeguard for Privileged Analytics compares actual user activity to user profiles in real time, and profiles are continually adjusted using machine learning. Safeguard for Privileged Analytics detects anomalies and ranks them based on risk so you can prioritize and take appropriate action and ultimately prevent data breaches.

Figure 1: Privileged Sessions and Privileged Passwords



Overview of the entities

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

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

Assets, partitions, and partition profiles

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

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

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

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

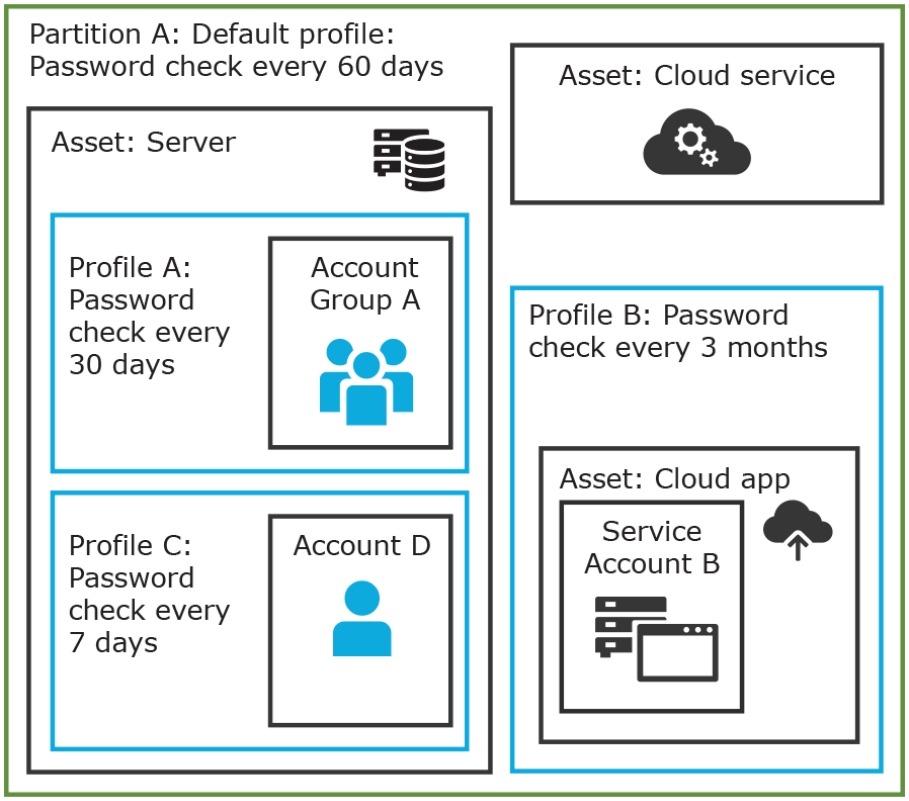
A partition can have multiple partition profiles, each assigned to different assets, if desired. An account is governed by only one profile. If an account is not explicitly assigned to a profile, the account is governed by the one assigned to the parent asset. If that asset does not have an assigned profile, the partition's default profile is assigned. When updating or restarting a service on a password change, the profile assigned to the asset is used for dependent account service modifications. For more information, see Adding change password settings in the *Safeguard for Privileged Passwords Administration Guide*.

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

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

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

Figure 2: Password control



Details: Assets and asset groups

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

Details: Partitions and partition profiles

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

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

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

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

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

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

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

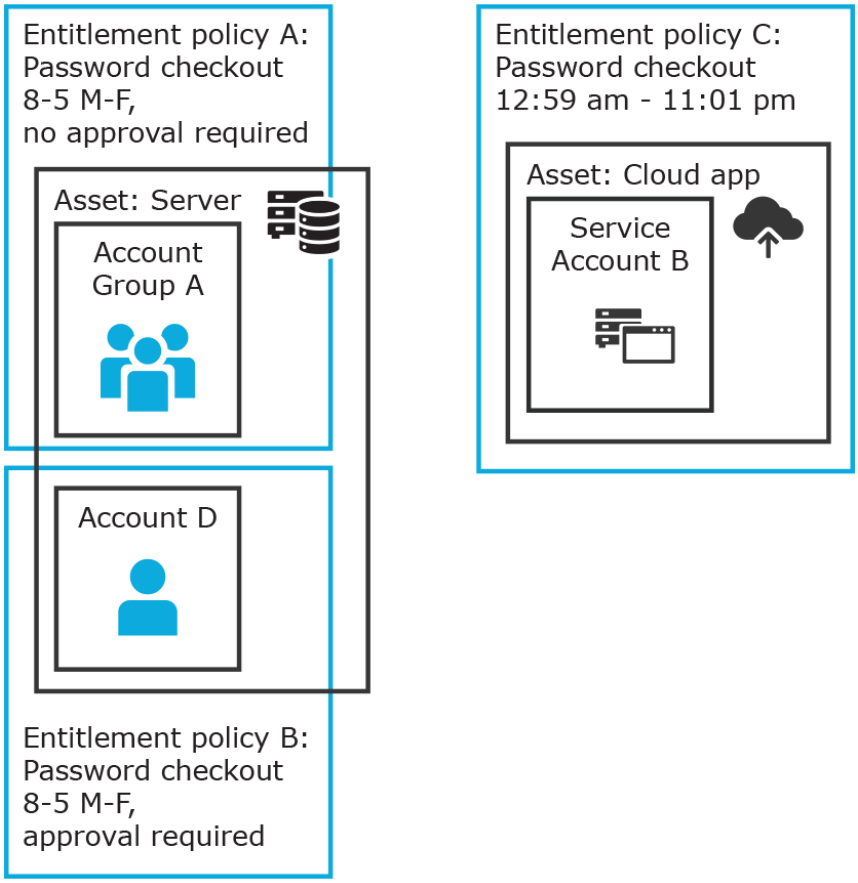
Entitlement access request policies may include:

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

In the example below, each account or account group is assigned to only one asset. The Server asset is associated with Account D and Account Group A which is made up of several accounts. Entitlement access request policy A is assigned to Account Group A so that group

can check out passwords from 8 a.m. to 5 p.m. on Monday through Friday with no approval required. Entitlement access request policy B, which is associated with Account D, allows for password check out for the same time frame, but the check outs require approvals. Entitlement access request policy C allows for password check out from 12:59 a.m. to 11:01 p.m. to allow for the system maintenance window.

Figure 3: Entitlements and accounts



Details: Accounts and account groups

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

Details: Entitlements and access request policies

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

Users and user groups

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

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

Users can be configured for two-factor authentication.

Details: Users and user groups

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

Discovery

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

Access request workflow

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

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

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

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

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

Key features

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

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

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.

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

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

Feature	Description
	• Last Name • Work Phone • Mobile Phone • Email • Description • External Federation Authentication • Radius Authentication • Managed Objects • Groups • Name • Members • Description
Discovery	Quickly discover any privileged account or system on your network with host , directory, and network-discovery options.
Event notification options	Safeguard for Privileged Passwords allows you to configure the appliance to send event notifications to external systems such as Email, Syslog, and SNMP.
Favorites	Quickly access the passwords that you use the most right from the Home screen. You can group several password requests into a single favorite so you can get access to all the accounts you need with a single click.
One Identity Starling	Expand the capabilities of Safeguard with One Identity Starling, which offers immediate access to cloud delivered features and services. This includes all-you-can-eat Starling Two-Factor Authentication (2FA) to protect Safeguard access.
Partitions and Profiles	Safeguard for Privileged Passwords allows you to group managed systems into secure work areas that can be designated for delegated management.
Release control	Manages password requests from authorized users for the accounts they are entitled to access via a secure web browser connection with support for mobile devices.
RESTful API	Safeguard for Privileged Passwords (SPP) is built with an API-first design and uses a modernized API based on a REST architecture that allows other applications and systems. Every function is exposed through the API to enable quick and easy integration regardless of what you want to do or which language your applications are written in. There are even a few things that can

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

Sessions key features

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

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

For more information, see SPP and SPS sessions appliance join guidance in the *Safeguard for Privileged Passwords Administration Guide*.

2

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.

- You may use the hardware appliance or virtual appliance:
  - Setting up the hardware appliance
  - Setting up the virtual appliance
- Completing the appliance setup
- Creating authorizor admin and local admin 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 *Safeguard for Privileged PasswordsAdministration Guide*.

Setting up the hardware appliance

CAUTION: To maximize security, restrict the access to MGMT interface to as few users as possible. The Management web kiosk gives access to functions without authentication, such as pulling a support bundle or rebooting the appliance.

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

Step 1: Before you start

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

Step 2: Prepare for installation

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

- Laptop
- IP address
- IP subnet mask
- IP gateway
- DNS server address
- NTP server address
- Safeguard for Privileged Passwords license

  If you purchased 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.

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 Safeguard for Privileged Passwords 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.

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 in to 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 in to the Safeguard for Privileged Passwords web client using the Bootstrap Administrator account:
   - User name: **admin**
   - Password: **Admin123**

   The Bootstrap Administrator is a built-in account that allows you to get the appliance set up for first-time use. To keep your Safeguard for Privileged Passwords Appliance secure, change the default password for the Bootstrap Administrator's account. For more information, see Completing the appliance setup on page 23.
4. Configure the primary network interface (X0): On the **Appliance Configuration** page, configure the following. Click the **Edit** icon to modify these settings.

- 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**.

5. Log in and download the desktop client to complete the next steps. For more information, see Completing the appliance setup on page 23.

Step 7: Connect the appliance to the network

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

Setting up the virtual appliance

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

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

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

Step 1: Make adequate resources available

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

Step 2: Deploy the VM

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

Hyper-V zip file import and set up

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

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

Step 3: Initial access

Initiate access using one of these methods:

- Via a virtual display: Connect to the virtual display of the virtual machine. You will not be offered the opportunity to apply a patch with this access method. Upload and download are not available from the virtual display. Continue to step 4. If you are using Hyper-V, make sure that Enhanced Session Mode is disabled for the display. See your Hyper-V documentation for details.
- Via a browser: Configure the networking of your virtual infrastructure to proxy https://192.168.1.105 on the virtual appliance to an address accessible from your workstation then open a browser to that address. For instructions on how to do this, consult the documentation of your virtual infrastructure (for example, VMWare). You will be offered the opportunity to apply a patch with this access method. Upload and download are available from the browser. Continue to step 4.

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

Step 4: Complete initial setup

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

Step 5: Log in and configure Safeguard for Privileged Passwords

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

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

          You can update this information in **Administrative Tools** | **Settings** | **Appliance** | **Operating System Licensing**. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Operating system license.

    c. **NTP**: Complete the Network Time Protocol (NTP) configuration.
        - Select **Enable NTP** to enable the protocol.
        - Identify the **Primary NTP Server** IP address and, optionally, the **Secondary NTP Server** IP address.
    d. **Network (X0)**: For the X0 (public) interface, enter the IPv4 and/or IPv6 information, and **DNS Servers** information.

5. Click **Save**. The virtual appliance displays progress information as it configures Safeguard, the network adapter(s), and the operating system licensing.
6. When you see the message `Maintenance is complete`, click **Continue**.

Step 6: Access the desktop client or use the web client

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

- (desktop client): Log in and download the desktop client. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Installing the desktop client.
- (web client): Use the web client. For more information, see the *Safeguard for Privileged Passwords Administration Guide*, Using the web client.

Step 7: Change the Bootstrap Administrator's password

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

View or change the virtual appliance setup

You can view or change the virtual appliance setup.

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

Completing the appliance setup

After setting up the hardware appliance or virtual appliance, complete these steps.

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

Step 1: Install the desktop client application and desktop player

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

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

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

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

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

Installing the Safeguard for Privileged Passwords desktop client application

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

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

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

Installing the Desktop Player

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

1. Once the Safeguard for Privileged Passwords installation is complete, go to the Windows **Start** menu, **Safeguard** folder, and click **Download Safeguard Player** to be taken to the One Identity Safeguard for Privileged Sessions - Download Software web page.
2. Follow the *Install Safeguard Desktop Player* section of the player user guide found here:

a. Go to One Identity Safeguard for Privileged Sessions - Technical Documentation.

b. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.

3. For Safeguard Desktop player version 1.8.6 and later, ensure your signed web certificate has a Subject Alternative Name (SAN) that includes each IP address of each of your cluster members. If the settings are not correct, the Safeguard Desktop Player will generate a certificate warning like the following when replaying sessions: `Unable to verify SSL certificate. To resolve this issue, import the appropriate certificates including the root CA.`

New Desktop Player versions

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

Step 2: Start the desktop client

1. Log in using the Bootstrap Administrator account.
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 Safeguard for Privileged Passwords using the provided license file. Go to **Licensing**:
   - (web client): Click **Settings** on the left. The **Settings: Appliance** page displays. Click **Licensing** .
   - (desktop client): Navigate to **Administrative Tools** | **Settings** | **Appliance** | **Licensing**.

   Click + to upload a new license file.
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.

Changing the Bootstrap Administrator's password

The Bootstrap Administrator is a built-in account that allows you to get the appliance set up for first-time use. To keep your Safeguard for Privileged Passwords Appliance secure, once the license is added, change the default password for the Bootstrap Administrator's account.

To change the password:

-  (web client): Click your user name in the upper-right corner of the screen and select **Change Password**.
-  (desktop client): Click your user name in the upper-right corner of the screen and select **My Account** then **Change Password**.

If this password is ever lost, you can reset it to the default of Admin123. See the *Safeguard for Privileged Passwords Administration Guide*, Admin password reset topic.

Step 3: 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 4: 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 back up your Safeguard for Privileged Passwords Appliance.

Step 5: Add a user with Authorizer administrative permissions

The Authorizer Administrator is responsible for granting administrative access to 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 6: Change the local security policy

Before 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 7: 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 authorizor admin and local admin 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 in to the Windows desktop client application as the Bootstrap Administrator.
2. From the **Home** page, navigate to **Administrative Tools** and select **Users**.
3. Add the following additional local administrator users.

   IMPORTANT: After creating, log out as the Bootstrap Administrator and log in as the Authorizer Administrator. It is recommended you disable the Bootstrap Administrator for security purposes.

Username	Password	Permissions	Description
AuthorizerAdmin (Log in as this user to create all other administrators.)	Test123	All	The administrator responsible for creating all other administrators
ApplianceAdmin	Test123	Appliance	The administrator responsible for configuring the appliance
AssetAdmin	Test123	Asset	The administrator responsible for adding and managing partitions,

Username	Password	Permissions	Description
			assets, and accounts
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, verify that 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 in to 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

Joining Starling

One Identity Starling Two-Factor Authentication (2FA) is a Software-as-a-Service (SaaS) 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. By joining with One Identity Starling, Safeguard for Privileged Passwords customers can take advantage of companion features from multiple Starling services, such as Starling Two-Factor Authentication and Starling Connect.

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 (2FA), allowing approvers to receive a notification through an app on their mobile device when an access request is submitted. The approver can then approve (or deny) access requests through their mobile device without needing access to the desktop or web application.

  Approval Anywhere is enabled when you join Safeguard for Privileged Passwords to One Identity Starling. As a Security Policy Administrator, you must define the Safeguard for Privileged Passwords users authorized to use Approval Anywhere.

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

NOTE: You must be an Organization Admin for the Starling organization in order to join Safeguard for Privileged Passwords with Starling.

NOTE: You must download the **Starling 2FA** app on your mobile phone to use the Approval Anywhere feature.

1. Log in to 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** | **Identity and 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 in to 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 one 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, set up 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

   - 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
Windows Server Accounts	Accounts for the Windows machines
Directory Server Accounts	Accounts for the Directory machines

   - 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.

Password release workflow exercise

Now that you have setup 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 in to a web client using a mobile device. If mobile devices are not available, have your users log in to the Safeguard for Privileged Passwords desktop client at their own workstations.

To start the web client

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 in to each instance as your Requester, Approver, and Reviewer users.

(web client) Test: Request password

As Joe, the Requester user, perform the following steps.

1. From the web client, click **Home** or **My Requests**, then click **New Request**.
    - If you have set up a Linux account and a Windows account, request a password from each.
2. Use the default access options.
    - Notice how the policy configuration changes the user experience.
3. Open **Requests** and review your pending requests.

Test: Approve password requests

(web client) Did you receive a notification on your mobile phone? You can approve the request from your mobile device without being logged in to Safeguard for Privileged Passwords. As Abe, the Approver user, click **Approvals** on the left of the page to complete the approval.

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

As Abe, the Approver user, perform the following steps.

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

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

Test: The password and check it in

As Joe, perform the following steps.

1. 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.
2. Select **Copy**.
3. Using the password in your copy buffer, log in to the test server.
4. Log out of the test server and return to the Safeguard for Privileged Passwords desktop.
5. Select **Check-In** to complete the password check out process for the password requests.

Test: Review a password release

As Ralph, the Reviewer, use the web client or desktop client:

(web client)

1. Click **Reviews**. Select the request.
2. Enter a comment.
3. Click to mark the selected request as reviewed.

(desktop client)

1. 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

As *Joe*, perform the following steps.

1. 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.
2. 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.
3. **Copy** the password so you can use it to manually log in to the remote asset/account.
4. After you have successfully logged in to the remote asset/account, log out of the test server and return to the Safeguard for Privileged Passwords desktop.
5. Select **Check-In**.

Test: Review a password release

1. As Ralph, perform the following:
    - In the web client **Reviews** and click to mark the selected request as reviewed.
    - In the desktop client:
        1. Open **Reviews** and review the requests that are waiting for your review.
        2. Select **Workflow** to view the transactions that took place as part of the request.
        3. 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. In the desktop client, 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 five 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. to 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 check out 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. to 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. In the desktop client, 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 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 check out 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 check out 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 check out 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.

4

Auditing exercises

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

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

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, and so on.) 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 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 then 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

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: 1. Enter a **Name** for the rule.

Tab	Description
	2. For the **Settings**, click **Add Condition** to define criteria, including the search scope in the directory, then click **OK**. 3. On the Asset Discovery Rule dialog, for **Connection Template**, leave the default of **None**. 4. For **Asset Profile**, use the default partition profile to govern the discovered assets. 5. 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 reenables 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** that 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 five 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.

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.com/.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to videos at www.YouTube.com/OneIdentity.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

Index