One Identity Safeguard for Privileged Passwords 2.8.1

User Guide

Legend

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

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

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

Safeguard for Privileged Passwords User Guide
Updated - September 2019
Version - 2.8.1

Contents

1

Introduction

The One Identity Safeguard for Privileged Passwords User Guide is intended for non-administrative users who are authorized to request, approve or review access requests. It provides detailed instructions for performing these tasks using the Safeguard for Privileged Passwords desktop client.

Introduction to One Identity Safeguard for Privileged Passwords

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

A Safeguard for Privileged Passwords virtual appliance is also available.

Safeguard privileged management software suite

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

The Safeguard products' unique strengths are:

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

The suite includes the following modules:

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

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

Overview of the entities

Safeguard for Privileged Passwords is a password, keys, and secrets vault to secure assets including computers, servers, network devices, directories, and applications. Two types of access may be granted to assets 1) passwords (including secrets) and 2) sessions.

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

Assets, partitions, and partition profiles

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

The partition is a container for delegated management for account passwords (including check and change). Partitions are also useful to segregate assets to various owners to

achieve Separation of Duties (SoD). Partitions allow you to set up multiple asset managers, each with the ability to define password guidelines for the managed systems in their own workspace. Typically you would partition assets by geographical location, owner, function, or by operating system. For example, you can group Unix assets in a partition and delegate the Unix administrator to manage it. Every partition should have a partition owner.

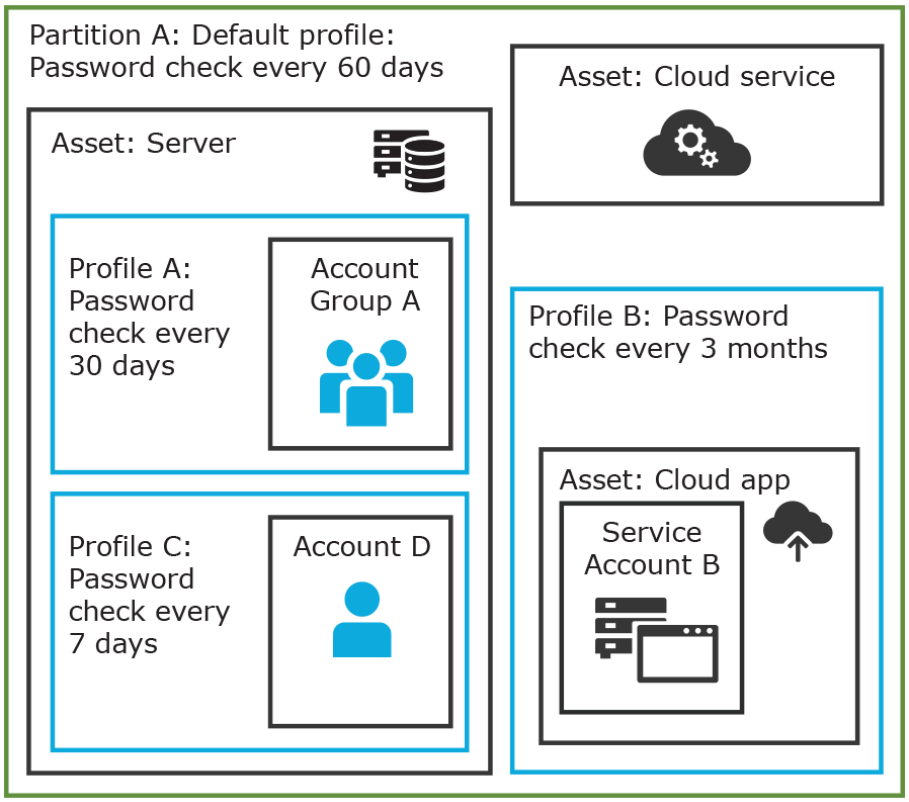
An asset can be assigned to only one partition at a time. When you assign an asset to a partition, all accounts associated with that asset are automatically reassigned to that partition, as well. Then, any new accounts you add for that asset are automatically assigned to that partition.

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

A partition can have multiple partition profiles, each assigned to different assets, if desired. An account is governed by only one profile. If an account is explicitly assigned to a profile, the account is governed by the one assigned to the parent asset. If that asset does not have an assigned profile, the partition's default profile is assigned.

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

For example, suppose you have an asset with 12 accounts and you configure the partition profile to check and change passwords every 60 days. If you want the password managed for one of those accounts every 7 days, you can create another profile and add the individual account to the new profile. Now, Safeguard for Privileged Passwords will check and change all the passwords on this asset every 60 days except for this account, which will change every 7 days.



In the example above, Partition A has three profiles (Profile A, B, and C) and a default profile. Profile A checks passwords every 30 days. Profile B checks passwords every 3 months, and Profile C has the highest level of security, checking passwords every 7 days. Note that the asset Server has two partition profiles each governing different accounts associated with the asset. Profiles A, B, and C are all explicitly assigned to the accounts and assets shown. Asset Cloud service doesn't have an explicitly assigned profile so the default will be used to manage accounts on the asset.

Details: Assets and asset groups

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

Details: Partitions and partition profiles

- A partition is a group of assets (and the assets' associated accounts) governed by a partition profile and used to delegate asset management. An asset can only be in one partition at a time. All accounts associated with that asset are automatically added to the partition.
- Partition profiles are the schedules and rules that govern a partition's assets and the assets' accounts. You can set a default partition profile to assign or you can manually assign a partition profile to an asset or account.
- When a partition is created, a default profile is created for that partition. This profile is implicitly associated with all assets and accounts added to the partition. Later, a different profile can be manually assigned to assets and account which is referred to as an explicit association. Explicit associations (manual assignments) override implicit associations (auto-assignments).

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

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

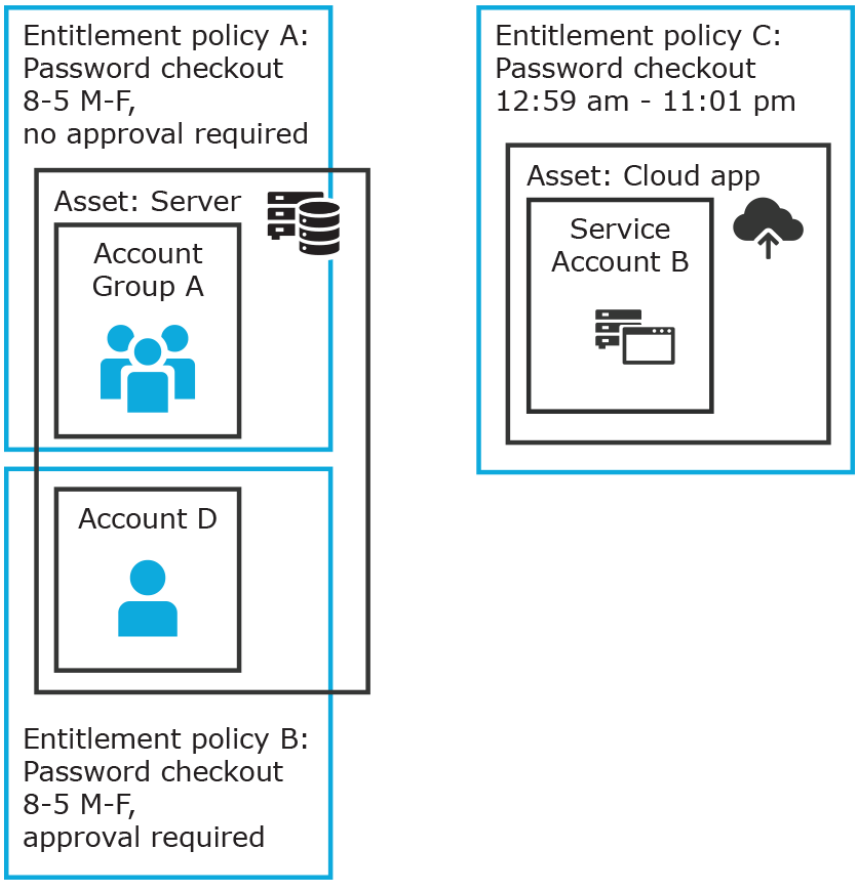
Entitlements grant access to users, user groups, or both. An entitlement includes one or more access request policies and may be related to job functions like help desk support or Unix administrators.

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

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

Entitlement access request policies may include:

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



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

Details: Accounts and account groups

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

Details: Entitlements and access request policies

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

Users and user groups

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

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

Users can be configured for two-factor authentication.

Details: Users and user groups

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

Discovery

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

Password request high level workflow

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

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

Session access

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

Key features

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

Table 1: One Identity Safeguard for Privileged Passwords key features

Feature	Description
Auto-login	Auto-login and sessions access request launch enhances security and compliance by never exposing the account credentials to the user.
Activity Center	Using the Activity Center, you can quickly and easily view all actions executed by Safeguard for Privileged Passwords users and integrated processes. Activity Center reports can be searched, customized and filtered to zero-in on the actions of a single user or to audit a variety of actions across a subset of departments. In addition, you can schedule queries, and save or export the data.
Always online	Safeguard for Privileged Passwords Appliances can be clustered to ensure high availability. Passwords and sessions can be requested from any appliance in a Safeguard for Privileged Passwords cluster. This distributed clustering design also enables the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
Approval Anywhere	Leveraging One Identity Starling, you can approve or deny any access request anywhere without being on the VPN.

Feature	Description

Directory integration	You can leverage your existing directory infrastructure (such as Microsoft Active Directory). You import directory users and directory groups. Directory users authenticate to Safeguard for Privileged Passwords with their directory credentials.
	
	Active Directory and LDAP data is automatically synchronized by asset or identity and authentication providers schema as shown in the following lists.
	
	Asset schema list
	
	• Users
	  • Username
	  • Password (modifiable in LDAP and not modifiable in Active Directory)
	  • Description
	• Groups
	  • Name
	  • Member
	• Computer
	  • Name
	  • Network Address
	  • Operating System
	  • Operating System Version
	  • Description
	
	Identity and Authentication Providers schema list
	
	• Users
	  • Username
	  • First Name
	  • Last Name
	  • Work Phone
	  • Mobile Phone
	  • Email
	  • Description
	  • External Federation Authentication
	  • Radius Authentication
	  • Managed Objects

Feature	Description

	• Groups
	  • Name
	  • Members
	  • Description

Discovery	Quickly discover any privileged account or system on your network with host , directory, and network-discovery options.
Event notification options	Safeguard for Privileged Passwords allows you to configure the appliance to send event notifications to external systems such as Email, Syslog, and SNMP.
Favorites	Quickly access the passwords that you use the most right from the Home screen.
Partitions and Profiles	Safeguard for Privileged Passwords allows you to group managed systems into secure work areas that can be designated for delegated management.
Release control	Manages password requests from authorized users for the accounts they are entitled to access via a secure web browser connection with support for mobile devices.
RESTful API	Safeguard for Privileged Passwords uses a modernized API based on a REST architecture which allows other applications and systems to connect and interact with it. The API enables quick and easy integration with diverse systems and applications spanning many programming languages.
Role-based access control (RBAC)	Safeguard for Privileged Passwords uses a role-based access control hierarchy using administrator permissions sets. Numerous roles are available for administrating Safeguard for Privileged Passwords enabling granular delegation and workflows along with least privileged access.
Secure access to legacy systems	Use smartcard, two-factor authentication or other strong authentication methods to gain access to systems. Because Safeguard for Privileged Passwords acts as a gateway or proxy to the system, it enables strong authentication to targets that cannot or do not support those methods natively.
Smartcard support	Authentication of your privileged users can be integrated with Microsoft's Active Directory support for Smartcards or manually uploaded to the Safeguard for Privileged Passwords Appliance itself.
Two-factor authentication support	Protecting access to passwords with another password isn't enough. Enhanced security by requiring two-factor authentication

Feature	Description
	to Safeguard for Privileged Passwords. Safeguard for Privileged Passwords supports any Radius-based 2FA solution and One Identity's Starling Two-Factor Authentication service.
Workflow engine	A workflow engine supports time restrictions, multiple approvers and reviewers, emergency access, and expiration of policy. It also includes the ability to input reason codes and/or integrate directly with ticketing systems. An access request can be automatically approved or require multiple sets of approvals.

Sessions key features

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

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

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

- Use Safeguard for Privileged Sessions via a join to Safeguard for Privileged Passwords.

  The join is initiated from Safeguard for Privileged Sessions. For details about the join steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Table 2: Key features using sessions

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

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

What's new in version 2.1

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

Table 3: Safeguard 2.1: Features and enhancements

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

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

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

What's new in version 2.2

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

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

Feature/Enhancement	Description
Additional platform support	Safeguard for Privileged Passwords now supports the management of assets on the following additional platforms: • FreeBSD • MongoDB • PostgreSQL • RACF - Mainframe LDAP • SAP HANA
Application to Application (A2A) integration	Using the Application to Application service, third-party applications can interact with Safeguard for Privileged Passwords in the following ways: • Credential retrieval: A third-party application can

Feature/Enhancement	Description
	retrieve a credential from the Safeguard for Privileged Passwords vault in order to perform automated functions on the target asset. In addition, you can replace hard coded passwords in procedures, scripts, and other programs with programmatic calls. • Access request broker: A third-party application can initiate an access request on behalf of an authorized user so that the authorized user can be notified of the available request and log in to Safeguard for Privileged Passwords to retrieve a password or start a session.
Asset administrator dashboard	The **Account Automation** tab on the **Dashboard** allows Asset and Directory administrators to view information regarding accounts that are failing different types of tasks, including: • Accounts where password check tasks failed. • Accounts where password change tasks failed. • Accounts where SSH key change tasks failed. • Accounts where suspend tasks failed. • Accounts where restore tasks failed.
Dynamic grouping and tagging	Dynamic grouping and tagging helps classify assets allowing Safeguard for Privileged Passwords to assign automatically provisioned systems and accounts to a policy. Tags allow Asset administrators to add additional metadata to accounts and assets to enrich the data on the object as it is added to Safeguard for Privileged Passwords. Tags can be dynamically added to assets and accounts based on tagging rules or they can be added manually. Policy administrators can create rules based on tags or from attribute information that is on the account or asset (for example, name, platform, partition, network address, and so on) to define group membership.
Event subscription	As a Safeguard for Privileged Passwords user, you can now control the email notifications you receive. Using the **Manage Email Notifications** control in your **My Account** pane, you can remove the events for which you do not want to receive email notifications. As a Safeguard for Privileged Passwords administrator, you can use the API to subscribe to the events for which you are interested in receiving notifications.

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

What's new in version 2.3

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

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

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

What's new in version 2.4

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

Custom platform (770747)

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

- Scripts:

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

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

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

Authentication options (765396)

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

Safeguard Sessions Appliance join (770739)

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

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

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

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

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

What's new in version 2.5

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

Directory based user discovery (713614 and 761638)

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

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

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

Offline Workflow (782735)

To ensure password consistency and individual accountability for privileged accounts, when an appliance loses consensus in the cluster access requests are disabled. In the event of an

extended network partition, the Appliance Administrator can manually place an appliance in Offline Workflow Mode to run access request workflow on that appliance in isolation from the rest of the cluster. When the network issues are resolved and connectivity is reestablished, the Appliance Administrator can manually resume online operations to merge audit logs, drop any in flight access requests, and return the appliance to full participation in the cluster.

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

What's new in version 2.6

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

Automatic Offline Workflow Mode (794644)

To reduce potential downtime, the Appliance Administrator can configure Offline Workflow Mode to be performed automatically. Offline Workflow Mode allows an appliance that has lost consensus (quorum) to operate in isolation from the cluster to process access requests using cached policy data.

To ensure the outage is not a short-lived outage, the default time before the appliance is automatically switched to Offline Workflow Mode is 15 minutes. The time threshold can be changed to 5 minutes or more.

If automatic Offline Workflow Mode is enabled, you can enable automatic Resume Online Workflow so the appliance automatically resumes online operations once consensus is restored. The minutes to wait after consensus is restored before automatically resuming online workflow defaults to 15 minutes. The time threshold can be changed to 5 minutes or more.

When Offline Workflow Mode settings are configured to run automatically, an Appliance Administrator can override the automatic settings and manually place an appliance in Offline Workflow Mode or manually restore an appliance to online workflow, as needed.

The user views status messages that clearly communicate the appliance state and the ability to request passwords.

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

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

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

Identity provider initiated single sign on flow (788935)

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

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

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

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

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

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

Restore a backup from a previous version (790917)

An Appliance administrator can restore backups as far back as Safeguard for Privileged Passwords version 2.2.0.6958. Only the data is restored; the running version is not changed.

If the administrator attempts to restore a version earlier than 2.2.0.6958, a message like the following displays: `Restore failed because the backup version '[version]' is older than the minimum supported version '2.2.0.6958' for restore.`

You cannot restore a backup from a version newer than the one running on the appliance. The restore will fail and a message like the following displays: `Restore failed because backup version [version] is newer then the one currently running [version].`

The backup version and the running version display in the Activity Center logs that are generated when Safeguard starts, completes, or fails a restore.

Service discovery (773722)

Overview

The Asset Administrator or delegated administrator can configure service discovery jobs to scan Windows assets and discover Windows services and tasks that may require

authorization credentials. If the Windows asset is joined to a Windows domain, the authorization credentials can be local on the Windows asset or be Active Directory credentials.

Running Service Discovery jobs

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

Discovered services and tasks association to known Safeguard accounts

Service discovery jobs associate Windows services and tasks with accounts that are already managed by Safeguard for Privileged Passwords. The accounts put under management display on the **Partitions** | **Discovered Services** tab as **Managed**. When the account's password is changed by Safeguard, Safeguard updates the password corresponding to the services or tasks on the asset according to the asset's profile change settings.

Service Discovery with Active Directory

A discovered service or task configured to use Active Directory authentication can be automatically linked to the asset with the account managed by Safeguard. Effectively, the asset will have an account dependency on the account.

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

Unmanaged accounts

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

View Service Discovery job status

From the Activity Center, you can select the Activity Category named Service Discovery Activity which shows the Event outcomes: **Service Discovery Succeeded**, **Service Discovery Failed**, or **Service Discovery Started**.

Session player installation (794597)

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

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

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

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

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

User experience if the Desktop Player is not installed

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

New Desktop Player versions

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

Time zone change (780266)

Safeguard for Privileged Passwords sets a default time zone based on the location and culture of the person performing the set up. The time zone is expressed as UTC + or – hours:minutes and is used for timed access (for example, access from 9 am to 5 pm). It is recommended that the Bootstrap Administrator set the desired time zone on set up. A User Administrator can also change the time zone.

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

What's new in version 2.7

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

Sessions Appliance join (792394)

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

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

The Asset Administrator can join a Safeguard for Privileged Sessions (SPS) cluster to a Safeguard for Privileged Password (SPP) cluster of one appliance or more for session recording and auditing. The actual join must be between the SPP primary and the SPS

cluster master. This means that the Safeguard for Privileged Sessions (SPS) cluster is aware of each node in an SPP cluster and vice-versa.

Once joined, all sessions are initiated by the SPP appliance via an access request and managed by the SPS appliance and sessions are recorded via the Sessions Appliance.

Session recording, playback, and storage

- Sessions recorded after the join are playable through SPP and are stored on the SPS appliance. An archive server can be set up through SPS.
- Sessions recorded prior to joining the Safeguard Sessions Appliances are not migrated to the SPS appliance. For that reason, it is recommended that the SPP sessions be migrated to an archive server prior to the join.

Safeguard for Privileged Passwords join guidance

Before initiating the join, review the steps and considerations in the join guidance.

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

Safeguard for Privileged Sessions join steps and troubleshooting

The join is initiated from Safeguard for Privileged Sessions. For details about the join steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

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

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

Overview

Safeguard for Privileged Passwords version 2.7, has been simplified to allow for a separation of duties based only on identity management, asset management, access policy configuration, and appliance maintenance. In the migration to version 2.7, greater flexibility is realized through these high-level assignments:

- Directories are migrated to assets.
- Accounts include both directory accounts and asset accounts.
- Each directory is assigned its own partition in the migration to version 2.7.

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

Administrators

- The Directory Administrator role is removed and users with Directory Administrator permission are assigned as partition owners for directories that are migrated to assets. This role does not include the ability to manage identity providers.

- An Authorizer administrator can now add an Active Directory forest only for identity to use as an unprivileged service account for connection.
- An Asset administrator can now:
    - Use service accounts to manage Active Directory. The service accounts can have limited permissions within a single domain.
    - Use multiple service accounts for managing the same Active Directory domain with different limited permissions within the domain. For example, the administrator can add the domain as a managed asset multiple times with different service accounts.
    - Use a service account from Active Directory to manage an asset from a different partition so that the administrator does not have to add that Active Directory to each of the administrator's partitions.
    - Set up a dependent system for a service running as an Active Directory account that isn't in the administrator's partition. This avoids having to add the Active Directory asset or the account to the partition.
    - Add Active Directory for authentication to Safeguard for Privileged Passwords without managing any of the accounts in Active Directory.
    - Set up multiple assets for the same domain.

Identity

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

Management

Directories can be subdivided so administrators can be assigned to manage portions of a directory. For example, Admin A might only manage objects in the Finance organizational unit (OU) of the directory and Admin B might only manage objects in the Engineering OU of the directory. This is possible via the settings on Assets including the asset **Name**, **Domain Name**, and whether to **Manage Forest**. This way, multiple assets can govern the same domain.

Directory accounts can be service accounts to other assets to run windows services/tasks on assets to keep password changes in sync.

Accounts

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

Assets

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

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

Discovery schedules

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

Account discovery enhancements (788930)

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

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

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

Activity Center enhancements (799288, 799308, 799307)

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

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

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

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

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

Asset discovery enhancements (782848)

Asset Administrators are now given:

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

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

Custom platform: TN3270 (798892)

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

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

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

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

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

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

Radius enhancements (798896)

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

- The User Administrator can choose to mask the Radius secondary authentication response entered by users by selecting the **Always Mask User Input** check box. If selected, the text box that the user enters their one-time password, or other challenge required by the Radius server, will always be a password style text box in which the user's input is masked and appears as a series of dots, not as clear text. This may be desired when the challenge is not just a one-time password, but also contains the user's PIN. This will prevent any passer-by from seeing the private information. Note, however, that when this setting is enabled, it will also override the Prompt attribute of the Radius server's Access-Challenge response, such that the user's input will always be masked.
- The User Administrator can choose to have the Radius secondary authentication pre-submit an Access-Request message to the Radius server in order to initiate a challenge/response cycle before the user sees or enters any information. The **PreAuthenticate for Challenge/Response** check box is used to indicate whether an Access-Request call containing only the User-Name should be sent to the Radius server prior to the user's authentication attempt. This is done to inform the Radius server of the user's identity so the server can possibly begin the authentication process by starting a challenge/response cycle. This may be required to seed the user's state data. In addition, the Radius server's response may include a login message that is to be displayed, which is specific to that user. Note, if the Radius server is not configured to respond with an Access-Challenge, then this will cause the log in to fail and the user will be unable to proceed.

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

What's new in version 2.8

One Identity Safeguard for Privileged Passwords introduces the following new features and enhancements in this version.

Virtual appliance and web management console (770749, 781091, 798013, 798014, 798527)

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

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

Security and backups

To maximize security in the absence of a hardened appliance, restrict the access to the Safeguard virtual disks, the web management console, and the MGMT interface to as few users as possible. Recommendations:

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

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

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

Application to Application (A2A) enhancement: API visible to certificate user (794148)

When registering a third-party application configured for credential retrieval, the Policy Administrator can make the registration, including the API keys, visible to the certificate user that is configured for the A2A registration. The third-party application can discover the API key and other information needed. The **Visible to certificate user** check box can be selected when adding an application registration via **Administrative Tools** | **Settings** | **External Integration** | **Application to Application**.

Custom platform: Telnet and HTTP support (799699, 787583)

Custom HTTP, SSH, Telnet, and TN3270 transports are available. For more information, see *Safeguard for Privileged Passwords Administration Guide*,Custom Platforms and Creating a custom platform script.

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

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

- Command-Reference:

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

https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/WritingACustomPlatformScript

- Example scripts platform scripts are available at this location:

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

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

Advanced password complexity rules (780274)

Separate password complexity rules can be set for local users and managed accounts. Password rules can be finely managed.

- Set the allowable password length in a range from 3 to 225 characters.
- Set first characters type and last character type.
- Allow uppercase letters, lowercase letters, numbers, and/or printable ASCII symbols along with the minimum amounts of each.
- Identify excluded uppercase letters, lowercase letters, numbers, and symbols.
- Identify if consecutive letters, numbers, and/or symbols can be repeated sequentially and, if allowed, set the maximum repetitions allowed.

Passwords are validated against the password rules before they are saved.

Job scheduler enhancements (753203)

An Appliance Administrator can finely tune backup and password check and change job schedules including the ability to ensure changes occur after hours. The administrator can create time windows including start and end times, days of the week, and days in a month by a static day of month or the first through fourth day of the month.

Safeguard for Privileged Sessions (SPS) initiated session (797262)

CAUTION: This functionality supports a future release of Safeguard for Privileged Sessions (SPS). For information on feature availability and use, see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Once the future release of SPS is joined to SPP, the Safeguard for Privileged Passwords (SPP) Asset Administrator can enable an SPS initiated session to get the session credentials from SPP.

- The administrator will navigate to **Administrative Tools** | **Settings** | **External Integration** | **Sessions Management** and set the **Session Module Password Access Enabled** toggle on or off. When the toggle is on (), SPS will create an access request and check out a password from SPP on behalf of another user. When the toggle is switched off (), this ability is revoked. (The toggle displays in SPP 2.8 but has no impact.)

  CAUTION: On the Session Settings tab, SPS Connection Policy, do not select `Sps initiated`. This is reserved for a future release of SPS if an access policy is used by SPS to create an SPS initiated access request.

Support for additional ServiceNow ticket types (793493)

System integrators designing privileged account access based on ServiceNow tickets can include ticket types for validation during access request workflow. The following tickets types are supported in addition to INC tickets:

- PRB (problem) tickets
- CHG (change) tickets
- RITM (request) tickets

If the ticket number is found in any of the ServiceNow tables searched (INC, CHG, RITM, or PRB) and the ServiceNow API property for the ticket is "Active", the user can make the access request.

Administrators can search by a ticket number in the Activity Center to find the access request.

2

System requirements

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

- The Windows desktop client consists of an end-user view and administrator view. The fully featured desktop client exposes all of the functionality of Safeguard based on the role of the authenticated user.
- The web client is functionally similar to the desktop client end-user view and useful for end-users requesting sessions and passwords.
- The web management console displays whenever you connect to the virtual appliance and is used for first time configuration.

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

If a Safeguard Sessions Appliance is joined to Safeguard for Privileged Passwords, session recording is handled via Safeguard for Privileged Session. The join is initiated from Safeguard for Privileged Sessions. For details about the join steps and issue resolution, see the *One Identity Safeguard for Privileged Sessions Administration Guide* at this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.

Bandwidth

We recommend that connection, including overhead, is faster than 10 megabits per second inter-site bandwidth with a one-way latency of less than 500ms. If you are using traffic shaping, you must allow sufficient bandwidth and priority to port 655 UDP/TCP in the shaping profile. These numbers are offered as a guideline only in that other factors could require additional network tuning. These factors include but are not limited to: jitter, packet loss, response time, usage, and network saturation. If there is any questions please contact One Identity Technical Support.

Desktop client system requirements

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

NOTE: The Windows desktop client also installs:

- Safeguard for Privileged Passwords PuTTY: Used to launch an SSH client if PuTTY is not available on the machine.

Table 6: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6 (or greater)
Windows platforms	64-bit editions of: • Windows 7 • Windows 8.1 • Windows 10 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 If the appliance setting, **TLS 1.2 Only** is enabled, (**Administrative Tools** | **Settings** | **Appliance** | **Appliance Information**), ensure the desktop client also has TLS 1.2 enabled. If the client has an earlier version of TLS enabled, you will be locked out of the client and will not be able to connect to Safeguard for Privileged Passwords. NOTE: Internet Explorer security must be set to use TLS 1.0 or higher. Ensure the proper "Use TLS" setting is enabled on the Advanced tab of the **Internet Options** dialog (In Internet Explorer, go to **Tools** | **Internet Options** | **Advanced** tab).
Desktop Player	See *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide* available at: One Identity Safeguard for Privileged Sessions - Technical Documentation, **User Guide**.

Web client system requirements

Table 7: Web client requirements

Component	Requirements
Web browsers	Desktop browsers: • Google Chrome 66 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or later) Mobile device browsers: • Apple Safari iOS 10 (or later) • Google Chrome on Android The web client is implemented for modern web browser technology, using: • HTML5 • CSS • JavaScript NOTE: If your browser lacks these required technologies, then use the desktop client.

Product licensing

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

Hardware appliance

The One Identity Safeguard for Privileged Passwords 2000 Appliance ships with the following module which requires a valid license to enable functionality:

- Privileged Passwords
- Privileged Sessions

You must install a valid license for each Safeguard for Privileged Passwords module to operate. More specifically, if any module is installed, Safeguard for Privileged Passwords will show a license state of **Licensed** and is operational. However, depending on which models are licensed, you will see limited functionality. That is, even though you will be able to configure access requests:

- If a Privileged Passwords module license is not installed, you will not be able to request a password release.
- If a Privileged Sessions module license is not installed, you will not be able to initiate a session access request from the embedded sessions module.

Virtual appliance licensing

The Safeguard for Privileged Passwords virtual appliance requires a valid Microsoft Volume License Agreement that includes licensing for Windows 10 Enterprise. Privileged sessions is available via a join to Safeguard for Privileged Sessions.

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

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

Installing the desktop client

To request, approve or review password releases, you must first install the desktop client application.

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

Installing the desktop client

NOTE: The install also includes: Safeguard for Privileged Passwords PuTTY which is used to launch the SSH client for SSH session requests.

Installing the Safeguard for Privileged Passwords desktop client application

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

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

   Save the **Safeguard.msi** file in a location of your choice.
2. Run the MSI package.
3. Select **Next** in the **Welcome** dialog.
4. Accept the **End-User License Agreement** and select **Next**.
5. Select **Install** to begin the installation.
6. Select **Finish** to exit the desktop client setup wizard.

Installing the Desktop Player

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

1. Once the Safeguard for Privileged Passwords installation is complete, go to the Windows **Start** menu, **Safeguard** folder and click **Download Safeguard Player** to be taken to the One Identity Safeguard for Privileged Sessions - Download Software web page.
2. Follow the *Install Safeguard Desktop Player* section of the player user guide found here:
    a. Click this link: One Identity Safeguard for Privileged Sessions - Technical Documentation.
    b. Scroll to **User Guide** and click *One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide*.

New Desktop Player versions

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

Starting the desktop client

The following steps assume the Safeguard for Privileged Passwords 2000 Appliance has been configured and licensed. As a Safeguard for Privileged Passwords user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

To start the desktop client application

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

    > NOTE: When entering an IPv6 address, enclose the IPv6 address in square brackets.

3. On the user login screen, enter your credentials and click **Log in**.
    - User Name: Enter your user or display name. Do not include spaces in the User Name.

        > NOTE: When using directory account credentials, enter your domain\name.

- Password: Enter the password associated with the user entered above.

4. If your Safeguard for Privileged Passwords user account requires you to log in with secondary authentication, enter the secure password token code, or other authentication for your authentication service provider account and click **Submit**.

   NOTE: The type and configuration of the secondary authentication provider (RSA SecureID, One Identity Starling Two-Factor Authentication, etc.) determines what you must provide for secondary authentication. Check with your system administrator for more information about how to log into Safeguard for Privileged Passwords with secondary authentication.

Uninstalling the desktop client

To uninstall the desktop client

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

4

The console

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

- Windows desktop client

  The desktop client consists of an end-user view and an administrator view. The administrative functionality is dynamically enabled based on the user's permissions.

- Web client

  The web client is functionally similar to the desktop client end-user view. It exposes the access request workflow functionality and is meant primarily for the non-administrative user. The web client uses a responsive UI design to adapt to the user's device -- from desktops to tablets or mobile phones.

Since the functionality of these two user interfaces are similar, this guide only describes the Windows desktop client.

Toolbar

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

- User avatar: Modify personal information, view notifications, or log out of the Safeguard client. For more information, see User information and log out on page 44.
- Settings: Configure the desktop client application, including notifications and Home page widgets, or view product information, including contact information.For more information, see Settings on page 42.

Settings

The Safeguard for Privileged Passwords console **Settings** (⚙) allows you to configure the desktop client application.

Notifications

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

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

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

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

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

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

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

Widgets

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

- Requests
- Approvals
- Reviews

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

About dialog tab

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

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

User information and log out

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

My Account

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

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

To update your personal information

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

To change your user password

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

To manage the notifications you receive

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

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

   NOTE: When there are no delegated owners assigned to a partition, email notifications related to partitions are sent to the Asset administrator. However, when a delegated owner is specified to manage the assets and accounts in a partition, email notifications related to partitions are sent to the delegated owner, not to the Asset administrator.
3. From this dialog, you can define the types of events for which you want to receive

notifications.

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

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

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

Log Out

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

5

Navigation pane

The **Home** page left navigation pane has these links.

- Home: Where you view and take action on the access request tasks that need your immediate attention. As a "requester" it also provides access to your list of "Favorite" access request queries.
- Dashboard: Where Security Policy Administrators can audit access requests. Where Asset Administrators can view information regarding accounts that are failing different types of tasks.
- Activity Center: Where you can search for and review activity for a specific time frame.
- Reports: Where you can view and export entitlement reports that show you which assets and accounts a selected user is authorized to access.
- Administrative Tools: Where you add all the objects you need to write access request policies, such as users, accounts, and assets. Where you define and management all of the administrative Safeguard for Privileged Passwords settings.

Home

When you log into Safeguard for Privileged Passwords, you begin on the **Home** page. The **Message of the Day** displays on the right side. The rest of the Home page is tailored to your user rights and permissions. If you are authorized by an entitlement to request, approve, or review access requests, then your Home page gives you a quick view to the access request tasks that need your immediate attention.

You can turn **Requests**, **Approvals**, and **Reviews** widgets on or off in Settings.

The Appliance Administrator sets the **Message of the Day**.

Requester's Home page view

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

For more information, see:

- Requesting a password release
- Requesting session access

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

For more information, see:

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

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

Favorites pane: Action bar buttons

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

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

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

Submit a favorite request

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

For more information, see:

- Creating, editing, or removing a favorite request

Approver's Home page view

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

For more information, refer to these topics:

- Approving a password release request
- Approving a session request

Reviewer's Home page view

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

For more information, refer to these topics:

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

Search box

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

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

Rules for using the search functionality:

- Search strings are not case sensitive.
- Wild cards are not allowed.
- Try using quotes and omitting quotes. As you use the product, you will become familiar with the search requirements for the search fields you frequent. Safeguard may perform a general search (for example, omits quotes) or a literal search (for example, includes quotes). Example scenarios follow:
    - On the Settings pane, search strings must be an exact match because a literal search is performed. Do not add quotes or underlines. For example, from the Settings pane, enter `password rules` to return **Safeguard Access | Password Rules**. If you enter **"password rules"** or **password_rules**, the

following message is returned: `No matches found`.

- On the Users pane search box:
  - A general search does not return anything if you use quotes because it uses a literal search (searches for the quotes). For example: searching for "ab_misc2" returns the message: `There is nothing to show here`.
  - You can use quotes in an attribute search if there are spaces in the search name. For example, entering the following in the search box **Username: "ab_misc2"** returns: `AB_misc2`.

- When multiple search strings are included, all search criteria must be met in order for an object to be included in the results list.
- When you combine a basic search and an attribute search, the order they are entered into the search box matters. The attribute searches can be in any order, but the basic search must come after the attribute searches.
- In large environments, you will see a result number to tell you how many objects match the criteria; however, only the first 200 objects will be retrieved from the server. When you scroll down the list, more objects will be retrieved (paged) as needed.

To search for accounts

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

   For example, enter **T** in the search box to search for items that contain the letter "T", or enter **sse** to list all items that contain the string "sse", such as "Asset".

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

2. To clear the search criteria, click **Clear**.

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

You can also Search by attributeSelect a drop-down to sort.

Search by attribute

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

API attributes can be searched

The drop-down menu lists a limited number of attributes that can be searched; however, you can perform an attribute search using the English name of any attribute as it appears in the API. Nested attributes can be chained together using a period (.). To see a list of all the attributes, see the API documentation. For information about the API, see How do I access the API.

Entering the search string

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

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

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

   You can specify multiple attributes, repeating these steps to add an additional attribute to the search box. Do not add punctuation marks, such as commas or colons to separate the different attributes. When multiple attributes are included, all search criteria must be met in order for an object to be included in the results list.

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

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

3. To clear the search criteria, click **Clear**.

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

Attributes in each Search box

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

Accounts

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

Account Groups

- Name
- Description
- Dynamic

Assets

- Name
- Description
- Platform
- Forest Root Domain

- Network Address
- Partition
- Is Directory
- Tag

Asset Groups

- Name
- Description
- Dynamic

Entitlements

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

Partitions

- Name
- Description

Users

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

User Groups

- Name
- Description

6

Privileged access requests

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

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

As a Safeguard for Privileged Passwords user, your **Home** page provides a quick view to the access request tasks that need your immediate attention. In addition, Safeguard for Privileged Passwords can be configured to alert you when you have pending tasks awaiting your attention. For more information, see Configuring alerts on page 55.

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

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

  Requesters can also define favorite requests, which then appear on their **Home** page for subsequent use. For more information, see Creating, editing, or removing a favorite request on page 53.
- Designated "approvers" see tasks related to approving (or denying) and revoking access requests.
- Designated "reviewers" see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

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

- Password release request workflow
- Session request workflow

Creating, editing, or removing a favorite request

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

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

To create a favorite request from your Home page

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

    Required

    b. **Description**: Enter descriptive text about the request.
    c. **Color**: Select the icon color to be used to display the request in your **Favorites** pane.

    Click **Add**.

    The dialogs will close and the new favorite will be added to the **Favorites** pane on your **Home** page.

To create a favorite request from the New Access Request dialog

1. At the bottom of the **New Access Request** dialog, click the **Add to Favorites** button when you are creating a new request. The **Add to Favorites** button is

enabled when you have selected the minimum required information (that is, at least one asset, account, and an access type) for the access request.

2. In the **Add to Favorites** dialog, specify the following:
    a. **Name**: Enter a name for the request.

       Required

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

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

To change a favorite request's icon color

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

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

To remove a favorite request

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

Configuring alerts

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

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

There are two ways to configure One Identity Safeguard for Privileged Passwords to send event alerts to Safeguard for Privileged Passwords users:

- Toast notifications Configure alerts that appear on your console when the desktop client application is not the active foreground application.
- Email notificationsConfigure email notifications.

Toast notifications

Toast notifications are alerts that appear on your console when the desktop client application is not the active foreground application; for example, when you are in another application or when you have minimized the One Identity Safeguard for Privileged Passwords desktop client.

To enable toast notifications

1. Open ⚙ Settings.
2. Select the **Enable Toast Notifications** check box.

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

Email notifications

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

- You must set your email address correctly in **My Accounts**. For more information, see User information and log out on page 44.
- Contact your Security Policy Administrator to ensure the access request policies are configured to notify people of pending access workflow events.
- Contact your Appliance Administrator to ensure the SMTP server is configured for email notifications.

Password release request workflow

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

Typically a password release request follows this workflow.

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

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

Requesting a password release

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

NOTE: You can configure One Identity Safeguard for Privileged Passwords to notify you of pending password release workflow events, such as when a password release request is pending, denied or revoked, and so forth. For more information, see Configuring alerts on page 55.

To request a password release

1. From your **Home** page, click **New Request** to open the **New Access Request** dialog.

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

2. On the **Asset Selection** tab, select the assets to be included in the access request.

   Limit: 50 assets

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

3. On the **Account & Access Type** tab, select the accounts to be included in the access request and the type of access being requested for each selected account. The accounts include linked accounts, if any. For more information, see Linked Accounts tab.

   - **Account**: The available account appears in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.
   - **Access Type**: The type of access request appears in the **Access Type** column. When multiple access request types are available, this value appears as a hyperlink, which when selected displays an additional dialog allowing you to select the access type. Select **Password Request**.

   To remove an asset or account from the list, select the entry in the grid and click the **Delete** toolbar button.

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

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

      NOTE: This option is only available if the policy has emergency access enabled.

   b. **Emergency Access**: Select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval.

      NOTE: This option is only available if the policy has emergency access enabled.

   c. **Request Immediately**: Clear this option to enter a specific date and time for the request.

      NOTE: Enter the time in the user's local time.

d. **Checkout Duration**: This either displays the checkout duration; or, if the **Allow Requester to Change Duration** option is enabled in the policy, it allows you to set the days, hours, and minutes that you want the password and overrides the checkout duration set in the access request policy.

e. **Ticket Number**: Enter a valid ticket number for this request.

> NOTE: Safeguard for Privileged Passwords does not display the **Ticket Number** option unless the Security Policy Administrator selected **Require Ticket Number** for this policy.
>
> When multiple accounts are specified in the request, if any of the selected accounts require a ticket number, you must specify a valid ticket number. The specified ticket number will be applied to all of the requests associated with this access request.

f. **Reason**: Select an access request reason code for this request.

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

> NOTE: Safeguard for Privileged Passwords does not display the **Reason** option unless the Security Policy Administrator selected reasons for this policy.
>
> When multiple accounts are specified in the request, if any of the selected accounts require a reason, you must specify a reason. The specified reason will be applied to all of the requests associated with this access request.

g. **Comment**: Enter information about this request.

Limit: 255 characters

> NOTE: When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request.

5. To save the access request as a favorite, click the **Add to Favorites** button.

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

   This access request is then added to your **Home** page **Favorites** pane. Selecting it from the **Favorites** pane displays the **New Access Request** dialog allowing you to edit the request details or enter a required reason or comment before submitting the request.

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

   The **Access Request Result** dialog displays showing you the access requests submitted and whether a request was successful.

Taking action on a password release request

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

To take action on a password release request

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

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

    NOTE: You enable or disable the **Home** page widgets in the Settings menu.
2. Open the list of requests and select one of the following view filters. The number indicates how many requests are in that state.
    - **All**: Requests in all states.
    - **Available**: Approved requests that are ready to view or copy.
    - **Approved**: Requests that have been approved, but the checkout time has not arrived.
    - **Pending**: Requests that are waiting for approval or for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
    - **Revoked**: Approved requests retracted by the approver.The approver can revoke a request between the time the requester views the password and checks it in.
    - **Expired**: Requests for which the checkout duration has elapsed.
    - **Denied**: Requests denied by the approver.
3. Select an account to see the details of the password release request.
4. Take the following actions on password release requests:
    - **Available**: Select **Copy** to checkout the password. This puts the password into your copy buffer, ready for you to use.

      Select **Check-In** to complete the password checkout process.

      Select **Show Password** to view the password on your screen. The password displays on your screen for 20 seconds.

      Selecting either **Copy** or **Show Password** constitute a password "checkout".

      If the password changes while you have it checked out, and your current request is still valid, select either **Copy** or **Show Password** again to obtain the new password.

      Select **Hide Password** to conceal the password from view.

- **Approved**: Select **Cancel** to remove the request.

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

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

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

Approving a password release request

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

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

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

You can configure Safeguard for Privileged Passwords to notify you of a password release request that requires your approval. For more information, see Configuring alerts on page 55.

To approve or deny a password release request

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

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

   NOTE: You enable or disable the **Home** page widgets in the Settings menu.
2. Open the list of approvals and select one of the following view filters. The number indicates how many requests are in that state.
   - **All**: Password release requests in all states.
   - **Pending**: Requests that are waiting for approval.

- **Approved**: Requests that have been approved, but not yet available to the requester.

3. Once you open the list, select the requester's name to see the details of the password release request.
4. Take the following actions on password release requests:
    - **Pending**: Select to **Approve** or **Deny** a password release request. Optionally, enter a comment of up to 255 characters.
    - **Pending Additional Approvers**: Select to **Deny** a password release request. Optionally, enter a comment of up to 255 characters.
    - **Approved**: Select to **Deny** or **Revoke** an approved request.

Reviewing a completed password release request

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

You can configure Safeguard for Privileged Passwords to notify you of a password release request that requires your review. For more information, see Configuring alerts on page 55.

To review a completed password release request

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

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

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

    Optionally, enter a comment of up to 255 characters.

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

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

Session request workflow

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

Typically a session request follows the workflow below:

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

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

About sessions and recordings

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

Important notes

- PuTTY is installed with the Windows desktop client and is used to launch the SSH client if PuTTY is not available on the machine.
- Sessions requests are enabled by default. However, if authorized users cannot request sessions, check the **Session Requests Enabled** setting (**Administrative Tools** | **Settings** | **Access Request** | **Enable or Disable Services**).

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

- All session activity (every packet sent and action that takes place on the screen, including mouse movements, clicks and keystrokes) is recorded and available for play back.
- If Safeguard for Privileged Passwords detects no activity for 10 minutes during a privileged session, the session is terminated.
- It is highly recommended to assign an archive server for each Safeguard Appliance's session recording to avoid filling up the appliance's disk space.

Embedded session related notes

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

- 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, set the following parameter: PasswordAuthentication yes.
- Both SSH and RDP session recordings use the Timestamping Certificate Authority.

  Recordings are signed and timestamped every 30 seconds so that partial recordings may be verified as authentic.
- During an RDP session, Safeguard proxies the connection to the target asset.

  When an RDP connection is established, the embedded sessions module will generate a certificate on the fly and sign it using the RDP Connection Signing Certificate. Therefore the RDP client trusts the RDP Connection Signing Certificate and the generated certificate that is signed by the RDP Connection Signing Certificate. This allows the client to verify that the connection is trusted.
- During an SSH session, Safeguard proxies the connection to the target asset. Therefore, Safeguard for Privileged Passwords's SSH host key (**Settings** | **Sessions** | **SSH Host Key**) must be trusted by the client. This SSH host key is unique and produced during manufacturing. This key can be trusted by the client or replaced with a different key if desired.

Requesting session access

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending access request workflow events, such as when a session request is pending, denied or revoked, and so forth. For more information, see Configuring alerts on page 55.

To request session access

1. From your **Home** page, click **New Request** to open the **New Access Request** dialog.

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

2. On the **Asset Selection** tab, select the assets to be included in the access request.

   Limit: 50 assets

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

3. On the **Account & Access Type** tab, select the accounts to be included in the access request and the type of access being requested for each selected account. The accounts include linked accounts, if any. For more information, see Linked Accounts tab.

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

     The accounts available for selection are based on the Asset-Based Session Access setting (Access Config tab) defined for the entitlement's access request policy. That is:

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

to select the access type. Select one of the following for a session request: **RDP** or **SSH**.

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

To remove an asset or account from the list, select the entry in the grid and click the − **Delete** toolbar button.

4. On the **Request Details** tab, configure the following settings, which will apply to all of the selected assets and accounts:
   a. **Normal Access**: (This option is only available if the policy has emergency access enabled.) Select this option to gain normal access to this password. Normal access ensures the access request goes through the entire end-to-end access release process from request to approval to review as defined in the policy by the Security Policy Administrator.
   b. **Emergency Access**: (This option is only available if the policy has emergency access enabled.) Select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval.
   c. **Request Immediately**: Clear this option to enter a specific date and time for the request. Enter the time in the user's local time.
   d. **Checkout Duration**: This either displays the checkout duration; or, if the **Allow Requester to Change Duration** option is enabled in the policy, it allows you to set the days, hours, and minutes that you want the password and overrides the checkout duration set in the access request policy.
   e. **Ticket Number**: Enter a valid ticket number for this request.

      Safeguard for Privileged Passwords does not display the **Ticket Number** option unless the Security Policy Administrator selected **Require Ticket Number** for this policy.

      When multiple accounts are specified in the request, if any of the selected accounts require a ticket number, you must specify a valid ticket number. The specified ticket number will be applied to all of the requests associated with this access request.
   f. **Reason**: Select an access request reason code for this request.

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

      Safeguard for Privileged Passwords does not display the **Reason** option unless the Security Policy Administrator selected reasons for this policy.

      When multiple accounts are specified in the request, if any of the selected accounts require a reason, you must specify a reason. The specified reason will be applied to all of the requests associated with this access request.
   g. **Comment**: Enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment,

you must enter a comment. The comment will be applied to all of the requests associated with this access request.

Limit: 255 characters

5. To save the access request as a favorite, click the **Add to Favorites** button.

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

   This access request is then added to your **Home** page **Favorites** pane. Selecting it from the **Favorites** pane displays the **New Access Request** dialog allowing you to edit the request details or enter a required reason or comment before submitting the request.

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

   The **Access Request Result** dialog displays showing you the access requests submitted and whether a request was successful.

Taking action on a session request

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

To take action on a session request

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

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

   NOTE: You enable or disable the **Home** page widgets in the Settings menu.

2. Open the list of requests and select one of these view filters:

State	Description
All	Requests in all states.
Available	Approved requests that are ready (that is, a session that can be launched).
Approved	Requests that have been approved, but the checkout time has not arrived.
Pending	Requests that are waiting for approval.
Revoked	Approved requests retracted by the approver.

State	Description
	The approver can revoke a request between the time the requester launches the session and checks it back in. When a user with Security Policy administrator permissions revokes a "live" session, the active session is terminated.
Expired	Requests for which the checkout duration has elapsed.
Denied	Requests denied by the approver.

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

3. Select an account to see the details of the session request.
4. You can take the following actions on session requests, depending on the state:

State	Actions
Available	Click ▶ **Launch** to launch the SSH client or Remote Desktop Connection. For more information, see Launching the SSH client or Launching an RDP session. Click ✓ **Check-In** to complete the checkout process once you have ended your session. In addition, you can use the following buttons to view or copy information into the configuration dialog that contains the credentials needed to launch the session: • **View**: Click this button to view the password or connection string, which is required to launch the session. • **Copy**: Click this button to copy a value to the copy buffer. • **Help**: Click this button to copy the value into the appropriate field of the configuration dialog. NOTE: The configuration dialogs are populated with the required information; these actions are available if the fields are not populated for some reason.
Approved	Click **Cancel** to remove the request. A sessions request changes from "Approved" to "Available" when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
Pending	Click **Cancel** to remove the request.

State	Actions
Revoked	Click **Resubmit Request** to request the session again. Click **Remove** to delete the request from the list.
Expired	Click **Remove** to delete the request from the list.
Denied	Click **Resubmit Request** to request the session again. Click **Remove** to delete the request from the list.

Approving a session request

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

You can configure Safeguard for Privileged Passwords to notify you of an access request that requires your approval. For more information, see Configuring alerts on page 55.

To approve or deny a sessions request

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

   NOTE: You enable or disable the **Home** page widgets in the Settings menu.

2. Open the list of approvals and select one of these view filters:

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

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

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

State	Actions
Pending	Select to **Approve** or **Deny** a sessions request. Optionally, enter a comment of up to 255 characters.
Pending Additional Approvers	Select to **Deny** a sessions request. Optionally, enter a comment of up to 255 characters.
Approved	Select to **Deny** or **Revoke** an approved request. You can revoke a request between the time the requester views it and checks it in. Any eligible approver can deny an access request after it has already been approved or auto-approved. Once disallowed, the requester will no longer be able to access the requested session, but he is given another opportunity to request that session again. The requester receives an email notifying him that the request was denied. For more information, see Configuring alerts on page 55.

Launching the SSH client

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

To launch the SSH client to begin your session

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Hostname Connection String) required to launch the SSH client.
2. Click the ▶ **Launch** button to the right of the asset name. Clicking this button displays the **PuTTY Configuration** dialog. The required information is populated, click **Open** to launch the SSH client.

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

a. Use the buttons to the right of the **Hostname Connection String** to perform the following tasks:

- **View**: To view the hostname connection string.
- **Copy**: To copy the value to your copy buffer, which can then be pasted into the Hostname field of the **PuTTY Configuration** dialog.
- **Help**: To copy the value into the Hostname field of the PuTTY Configuration dialog.

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

- **View**: To view the password.
- **Copy**: To copy the password to your copy buffer, which can then be pasted into the Password field of the **PuTTY Configuration** dialog.
- **Help**: To copy the value into the Password field of the **PuTTY Configuration** dialog.

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

3. In the SSH client, run the commands or programs on the target host.

   If there is no activity in an open session for about 10 minutes, the session will be terminated. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.

4. Once you are completed, log out of the target host and select **Check in** to complete the session request process.

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

Launching an RDP session

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

To launch a remote desktop connection to begin your RDP session

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Username Connection String) required to launch the remote desktop session.
2. Click the ▶ **Launch** button to the right of the asset name. Clicking this button displays the **Remote Desktop Connection** dialog. Click **Connect** to launch the remote desktop session.

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

   a. Use the buttons to the right of the **Username Connection String** to perform the following tasks:
      - **View**: To view the username connection string.
      - **Copy**: To copy the value to your copy buffer, which can then be pasted into the Username field of the **Remote Desktop Connection** dialog.
      - **Help**: To copy the value into the Username field of the **Remote Desktop Connection** dialog.

   b. Use the buttons to the right of the **Password** to perform the following tasks:
      - **View**: To view the password.
      - **Copy**: To copy the password to your copy buffer, which can then be pasted into the Password field of the **Remote Desktop Connection** dialog.
      - **Help**: To copy the value into the Password field of the **Remote Desktop Connection** dialog.

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

3. In the remote desktop session, run the commands or programs on the target host.

   NOTE: If there is no activity in an open session for about 10 minutes, the session will be terminated. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.

4. Once you are completed, log out of the target host and select ✔ **Check in** to complete the session request process.

   This makes the session request available to reviewers. If the **Record Sessions** option is enabled in the policy, the reviewer can play back the recording as part of the review process. In addition, if the **Enable Window Title Detection** option is selected in the policy, the reviewer can view a list of the windows opened on the desktop during the session.

Reviewing a session request

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

NOTE: You can configure Safeguard for Privileged Passwords to notify you of an access request that requires your review. For more information, see Configuring alerts on page 55.

To review a completed sessions request

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

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

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

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

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

        CAUTION: **If you receive a message like:** `No Desktop Player. The Safeguard Desktop Player is not installed. Would you like to install it now?`, **click Yes. See Installing the desktop client, Installing the Desktop Player, step 2.**
      - If **Enable Command Detection** is enabled in the policy, expand to show the details and click the **events** link on the Initialize Session event to view a list of the commands and programs run during the session.

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

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

Optionally, enter a comment of up to 255 characters.

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

Desktop Player User Guide

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

Replaying a session

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

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

To play back a session (Request Workflow dialog)

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

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

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

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

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

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

3. Accept the certificate to continue.

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

4. Use one of the following methods to play back the session recording:

- Click ▶ **Play Channel** from the toolbar at the top of the player.
- Click ▶ in the thumbnail in the upper right corner of the Information page.
- Click ▶ **Play Channel** next to a channel in the Channels pane.

Desktop Player User Guide

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

Archiving session recordings

About us

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

Contacting us

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

Technical support resources

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

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

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

Index

L

P

R

S

T

U

W