One Identity Safeguard for Privileged Passwords 7.0.5 LTS

User Guide

Contents

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 in Safeguard for Privileged Passwords.

Introduction to One Identity Safeguard for Privileged Passwords

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

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

Safeguard privileged management software suite

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

The Safeguard products' unique strengths are:

- One-stop solution for all privileged access management needs
- Easy to deploy and integrate

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

The suite includes the following modules:

- **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 to integrate seamlessly into existing networks. It captures the activity data necessary for user profiling and enables full user session drill-down for forensics investigations.

- **One Identity Safeguard for Privileged Analytics** integrates data from Safeguard for Privileged Sessions to use as the basis of privileged user behavior analysis. Safeguard for Privileged Analytics uses machine learning algorithms to scrutinize behavioral characteristics, and generates user behavior profiles for each individual privileged user. Safeguard for Privileged Analytics compares actual user activity to user profiles in real time, and profiles are continually adjusted using machine learning. Safeguard for Privileged Analytics detects anomalies and ranks them based on risk so you can prioritize and take appropriate action and ultimately prevent data breaches.

Figure 1: Privileged Sessions and Privileged Passwords
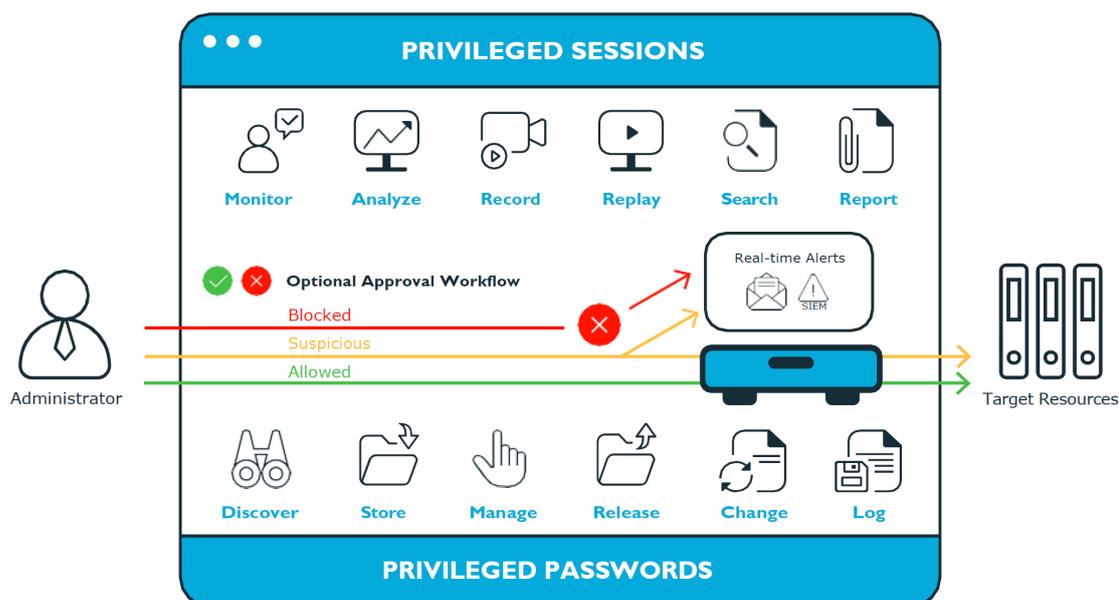
Overview of the entities

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

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

Assets, partitions, and profiles

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

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

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

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

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

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

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

Figure 2: Password control
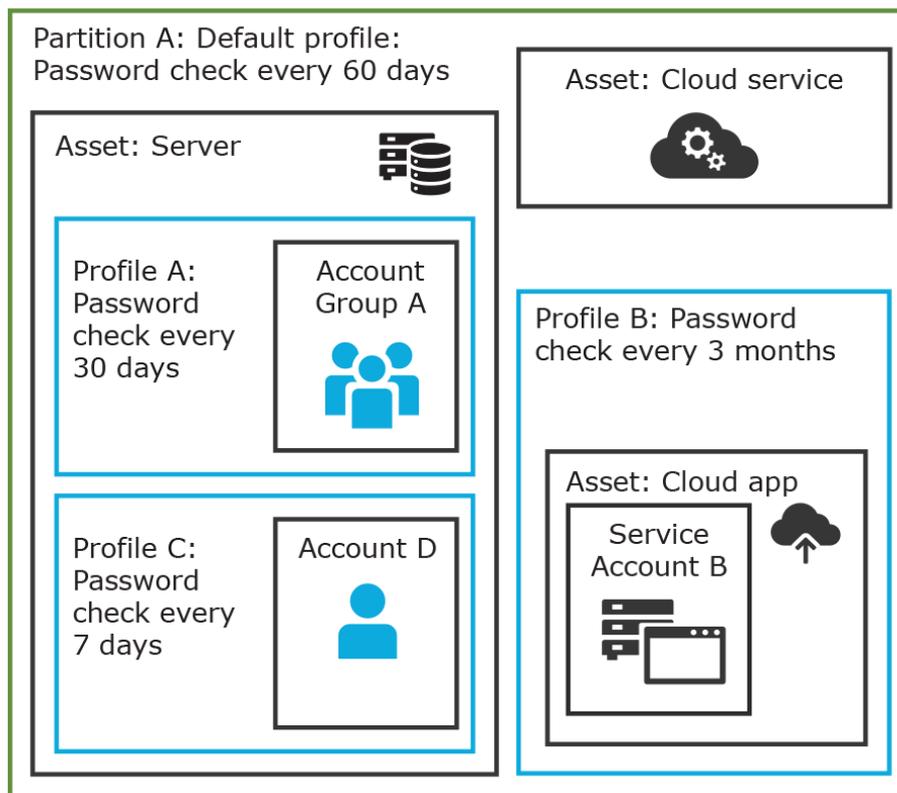
Details: Assets and asset groups

- An asset may be a computer, server, network device, directory, or application.

- You can log in to an asset with more than one account, but an account can only be associated with one asset.

- If you select an asset for a profile, all accounts are included.

- An asset must be assigned to only one partition. An asset typically has a profile, but it is not mandatory.

- You can create multiple assets for the same device or application then manage different accounts on each asset. For example, a directory asset can manage a subset of the forest.

- An asset group is a set of assets that can be added to the scope of an entitlement's access request policy.

Details: Partitions and profiles

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

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

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

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

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

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

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

Entitlement access request policies may include:

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

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

Figure 3: Entitlements and accounts
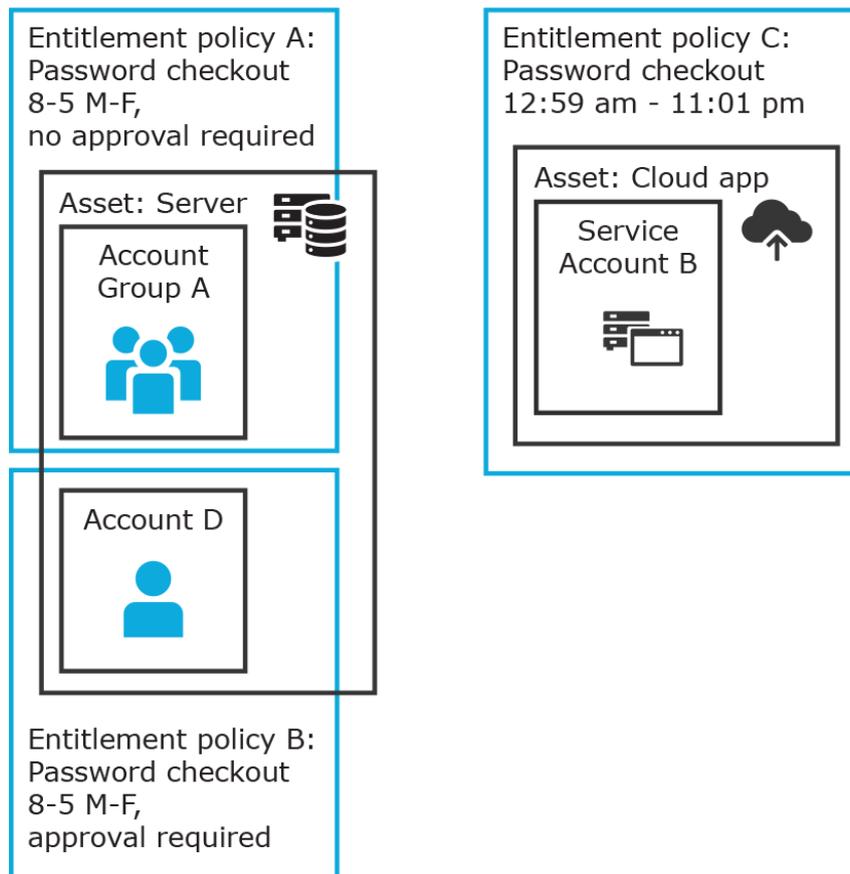
Details: Accounts and account groups

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

Details: Entitlements and access request policies

- An entitlement is a set of access request policies that restrict resources, typically by job role.

- Entitlements are used to authorize users or members of user groups to access accounts in the scope of the set of the entitlement's access request policies. One entitlement may have zero, one, or multiple access request policies. Users and user groups can be added to entitlements.

- Access request policies contain the details of the type of access as well as conditions. For example, the type of access may include password versus session (RDP session, SSH client, other protocols), time limits, individual accountability (change after check-in), and other settings. Conditions may include number of approvers, time of day, ticketing system, reason codes, and so on. An access request policy can only be associated with one entitlement.

- Access request policies are scoped to resources. Sometimes that scoping is done directly to accounts and the asset is implied. Or, the scoping is done to the asset and the access request policy identifies the account.

Users and user groups

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

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

Users can be configured for two-factor authentication.

Details: Users and user groups

- A user is a person who can log into Safeguard for Privileged Passwords. A user can be associated with an identity provider that is local or a user can be a directory user from an external identity store such as Microsoft Active Directory. A user may be associated with user groups, partitions, entitlements, and linked accounts.

- A user group is a set of users that can be added to an entitlement, typically based on roles. The user group's access is governed by the entitlement's access request policies. Both local user groups and directory user groups can be added to Safeguard for Privileged Passwords.

- A user can be assigned administrative permissions over assets, security, and so on. A standard user has no administrative permissions and performs other duties, for example, to approve access requests.

Discovery

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

Access request workflow

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

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

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

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

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

System requirements and versions

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

- The web client consists of an end-user view and administrator view. The fully featured client exposes all of the functionality of Safeguard based on the role of the authenticated user.

- The web management console displays whenever you connect to the virtual appliance and is used for first time configuration.
  When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. See One Identity's Product Support Policies for more information on environment virtualization.

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

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

Bandwidth

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

Web client system requirements

Table 1: Web requirements

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

Web management console system requirements

Table 2: Web kiosk requirements

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

Platforms and versions follow.

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

ONE IDENTITY
by Quest

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

Supported platforms

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

Safeguard for Privileged Passwords tested platforms

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

SPP linked to SPS: Sessions platforms

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

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

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

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

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

Table 3: Supported platforms: Assets that can be managed

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

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

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

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

Platform Name	Tested Versions	Supports SPP	Supports SPS Access
RACF - RACF - Mainframe LDAP	RACF - Mainframe LDAP z/OS V2.1 Security Server zSeries	True	False
	RACF - RACF - Mainframe LDAP z/OS V2.2 Security Server zSeries		
	RACF - RACF - Mainframe LDAP z/OS V2.3 Security Server zSeries		
Red Hat Enterprise Linux (RHEL)	Red Hat Enterprise Linux (RHEL) 7	True	True
	Red Hat Enterprise Linux (RHEL) 8		
	Red Hat Enterprise Linux (RHEL) 9		
Red Hat Directory Server	Red Hat Directory Server 11	True	False
	Red Hat Directory Server 12		
SAP HANA	SAP HANA	True	False
	SAP HANA 2		
SAP Netweaver Application Server	SAP Netweaver Application Server 7.5	True	False
Solaris	Solaris 10	True	True
	Solaris 11.3		
	Solaris 11.4		
SonicOS	SonicOS 6.5	True	False
	SonicOS 7		
	SonicOSX 7		
SonicWALL SMA or CMS	SonicWALL SMA or CMS 11.3.0	True	False
SQL Server	SQL Server 2014	True	False
	SQL Server 2016		
	SQL Server 2017		
	SQL Server 2019		
	SQL Server 2022		
SUSE Linux Enterprise Server (SLES)	SUSE Linux Enterprise Server (SLES) 12	True	True
	SUSE Linux Enterprise Server (SLES) 15		
Sybase (Adaptive	Sybase (Adaptive Server Enterprise)	True	False

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

Table 4: Supported platforms: Directories that can be searched

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

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

Custom platforms

The following example platform scripts are available:

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

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

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

- Command-Reference:

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

- Writing a custom platform script:

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

- Example platform scripts are available at this location:

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

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

Licenses

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

Hardware appliance

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

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

Virtual appliance Microsoft Windows licensing

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

Licensing setup and update

To enter licensing information when you first log in

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

On the virtual appliance, the license is added as part of Initial Setup.

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

To configure reminders for license expiration

To avoid disruptions in the use of Safeguard for Privileged Passwords, the Appliance Administrator must configure the SMTP server, and define email templates for the `License Expired` and the `License Expiring Soon` event types. This ensures you will be notified of an approaching expiration date.

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

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

To update the licensing file

Licensing update is only available using a virtual machine, not via the hardware.

To perform licensing activities

Go to the licensing page:

1. Navigate to **Appliance** > **Licensing**.

    - To upload a new license file, click **+Upload new license file** and browse to select the current license file. The Software Transaction Agreement will also be displayed during this process and must be read and accepted in order to complete the licensing process.

    - To remove the license file, select the license and click 🗑**Remove selected license**.

Long Term Support (LTS) and Feature Releases

Releases use the following version designations:

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

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

Table 5: Comparison of Long Term Support (LTS) Release and Feature Release

	Long Term Support (LTS) Release	Feature Release
General Release	**Scope**: Includes new features, resolved issues and security updates	**Scope**: Includes the latest features, resolved issues, and other updates, such as security patches for the OS
	Versioning: The first digit identifies the LTS and the second digit is a 0 (for example, 6.0 LTS, 7.0 LTS, and so on).	**Versioning**: The first digit identifies the LTS and the second digit is a number identifying the Feature Release (for example, 6.6, 6.7, and so on).
Maintenance Release	**Scope**: Includes critical resolved issues	**Scope**: Includes highly critical resolved issues
	Versioning: A third digit designates the maintenance LTS Release (for example, 6.0.6 LTS).	**Versioning**: A third digit designates the maintenance Feature Release (for example, 6.6.1).

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

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

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

Moving between LTS and Feature Release versions

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

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

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

Patching

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

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

Using the web client

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

To log into the web client application

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

1. From your browser, enter the Safeguard for Privileged Passwords URL with the IP address, such as `https://11.1.111.11`.

2. If a login notification displays, click **OK** to accept the notifications and restrictions stated.

3. On the user log in screen, enter your credentials and click **Log in**.

Updating your avatar photo

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

Using the left navigation menu

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

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

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

My Settings

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

Go to My Settings

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

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

Using the ⚙ General tab

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

Using the 🖥 My Account tab

- **Contact Information:** Click 🖉 **Edit** to change **Email**, **Work Phone**, or **Mobile Phone**. Click ✔ **Save** to save your changes or click ✖ **Cancel** to revert to the previous setting.

- **Location**: Select your time zone in the drop-down box. Changing your time zone may be prohibited based on your organization's security procedures. If available, choose to:
  - **Display times in local computer time**: This is the default. It is the time zone set on your local computer.
  - **Display times in my configured time zone**: This is the time zone that is set on this page.

- **Manage Email Notifications**: The **Manage Email Notifications** dialog displays the type of events for which you are receiving email notifications. You can define the types of events for which you want to receive notifications. By default, all events are selected. If the event is **Built In** to SPP, a ✔ displays. When there are multiple events, an **Events** link appears that leads to the **Subscriptions** dialog listing the **Name**, **Description**, and **Category** of the event.
  - Clear the check box for any events for which you do not want to receive an email notification.
  - To set all check boxes, select or clear the check box at the top of the list to the left of the header.

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

Asset Administrator.

- **Manage FIDO2 Keys** (Available if you are required to perform FIDO2 two-factor authentication.): If the FIDO2 feature is enabled, at least one FIDO2 key must be registered. When a key is added, the placeholder name is **Unnamed Key**. You can enter a meaningful name or later edit the name. It is recommended that all users have more than one key registered in case a key is lost or damaged. For existing keys, you will see the name and date each existing key was registered and last used.

  - To change a name, enter the new name, then click 💾 **Save**.

  - To remove a key, click ➖ **Remove** by the key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.

  - To add a key, click ➕ **Register New FIDO2 Key**.

    a. You will be asked to insert or connect to the new key.

    b. You will be prompted to reenter your primary credentials for verification.

    c. Tap or activate your new FIDO2 key that is being registered.

    d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name, then click 💾**Save**.

  For more information, see Requiring user to log in using secondary authentication.

- **Change Password**: The password requirements are listed. Enter your **Current Password** and the **New Password** as directed. (Click 👁**Display** or ⊘**Hide** to view or hide the password as it is entered.) Click **Save**.

Change password

You can change your password.

To change the password

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

FIDO2 keys

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

1. In the upper right corner, next to your user name, click ▼ .
2. Click **My Settings**.
3. Open the **My Account** tab.
4. Click **Manage FIDO2 Keys**. For existing keys, you will see the name and date each existing key was registered and last used.
5. Perform an action:

    - To change a name, enter the new name, then click 💾 **Save**.

    - To remove a key, click ⊖ **Remove** by the key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.

    - To add a key, click ➕ **Register New FIDO2 Key**.
        a. You will be asked to insert or connect to the new key.
        b. You will be prompted to reenter your primary credentials for verification.
        c. Tap or activate your new FIDO2 key that is being registered.
        d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name, then click 💾 **Save**.

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

Application switcher

Accessible from the toolbar, the application switcher allows you to navigate between One Identity products related to Safeguard for Privileged Passwords.

To use the application switcher

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

Log out

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

To log out

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

Search box

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

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

Rules for using the search functionality:

- Search strings are not case-sensitive. Exception: the Approvals and Reviews searches are case sensitive.

- When you click on the search icon in the search bar you will see a drop down of available search attributes (columns) for the grid. This can be used in conjunction with the entered search strings.

  Some of the search attributes will also have an arrow to expand subsearches. These subsearches have pre-defined search strings.

- By default, results are displayed in alphabetical order.

- 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 **Appliance Management** > **Search**, search strings must be an exact match because a literal search is performed. Do not add quotes or underlines. For example, from the Settings pane, enter `password rule` to return **Safeguard Access** > **Local Password Rule**. If you enter **"password rule"** or **password_rule**, the following message is returned: `No matches found`.

- On the Users pane search box, you can use quotes in an attribute search if there are spaces in the search name. For example, entering the following in the search box **Username: "ab misc2"** returns: `AB misc2`.

- When multiple search strings are included, all search criteria must be met in order for an object to be included in the results list. In the web client, if conflicting attributes are entered for the same search (for example, both true and false) then the results will expand to show all matches so long as they fit one of those attributes.

- When you combine a string search and an attribute search, the order they are entered into the search box matters. The attribute searches can be in any order, but the string search must come after the attribute searches.

- To search using dates and times in the web client, the following format is used: `YYYY-MM-DDThh:mm:ss`. For example, if you are searching for an entitlement that expires December 1, 2021 then you would use the following search: `ExpirationDate:2021-12-01`. To include a minimum and maximum value in a search, use `..` to separate two values. For example, if you are searching for an entitlement that expires between December 1, 2021 and December 3, 2021 then you would use the following search: `ExpirationDate:2021-12-01..2021-12-03`.

To search for objects or object details

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

   Examples:

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

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

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

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

You can also Search by attribute.

Search by attribute

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

API attributes can be searched

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

Entering the search string

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

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

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

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

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

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

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

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

Exporting data

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

To export data

1. Navigate to the page displaying the information to be exported. For example, if you want to export user information in order to see who can log into the product then you would navigate to the **Users** page.

2. (Optional) Apply filters or search criteria to the displayed data.

3. Click the 🔀 **Export** button.

4. On the export dialog, select **CSV** or **JSON**. Different information may be available depending on your selection. For example, when the data covers an array of information then the CSV will only report the number of items in the array whereas the JSON will contain the full list. This can be seen when exporting Account Groups data; the CSV will show the number of accounts in a group, but the JSON will show all of the information for all the accounts in a group.

5. Click **Fields** to open the **Export Fields** dialog where you can select which fields to include in the report. The **Export Fields** dialog will be prepopulated with the selections made during the last export of data from the page.

6. Click **OK** to save your selection.

7. Click **Sort By** to open the **Export Sort Order** dialog where you can select the order in which to sort the previously selected fields. This allows you to organize the exported data according to your needs.

    - ✚**Add Sort Order**: Use this button to add additional fields by which to sort the data.

    - ✖ **Clear All Sort Orders**: Use this button to clear all selected fields.

    - ⠿ **Drag up or down to change the sort order**: When you have multiple sort orders, click and hold this icon with your cursor then drag the selected sort order to whichever spot in the list you want.

    - **Order By**: Use this drop-down to select a field by which to sort the data.

        Additional drop-downs are added using the ✚**Add Sort Order** button. The **Order By** fields will be prepopulated with the selection(s) made during the last export of data from the page.

    - ⬆ or ⬇ **Change Sort Direction**: Clicking this button changes the sort direction for the field. For example, if you have selected FirstName in the

        Order By drop-down and ⬆ as the sort direction, your exported data will order the results in alphabetical order based on FirstName.

    - ➖ : Clicking this button removes the associated **Order By** selection.

8. Click **OK** to save your selection.

9. Selecting the **Limit Results** check box displays the **Number of results to include** field which is used to limit the number of results that will be included in the exported file. The **Number of results to include** field will be prepopulated with the selection made during the last export of data from the page.

10. Click **Export**.

Privileged access requests

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

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

As a Safeguard for Privileged Passwords user, your ♠ **Home** page provides a quick view to the access request tasks that need your immediate attention. In addition, an Administrator can set up alerts to be sent to users when there are pending tasks needing attention. For more information, see Configuring alerts on page 35.

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

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

  Requesters can also define favorite requests, which then appear on their ♠ **Home** page for subsequent use.

- Approvers see tasks related to approving (or denying) and revoking access requests.

- Reviewers see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

The following three workflows are available:

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

Configuring alerts

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

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

Email notifications

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

- For Local users, you must set your email address correctly in **My Settings**. For more information, see My Settings.
- For Directory users, set your email correctly in the directory where your user resides.
- 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 managed 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.

Requesting a password release

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending password release workflow events, such as when a password release request is pending, denied, or revoked, and so forth. For more information, see Configuring alerts on page 35.

To request a password release

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

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

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

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

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

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

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

- **Access Type**: The type of access request appears in the **Access Type** column. If the type is a drop-down, multiple access request types are available. Open the drop-down and select the access type, for example, **Password**, **RDP**, **SSH**, **SSH Key**, or **Telnet**.

- **Account Description**: (When applicable) The description of the account.

- **Asset Description**: (When applicable) The description of the asset.

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

3. Click **Next**.

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

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

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

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

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

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

      - View the **Checkout Duration**.

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

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

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

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

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

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

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

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

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

When the request has been approved, you can use the password. For more information, see Taking action on a password release request on page 38.

Taking action on a password release request

The actions that can be taken on a password release request depends on the state of the request and the client interface you are using.

To take action on a password release request

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

   • Click ![icon] then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.

   • Click **Sort By** ![icon] then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.

   • Click ![icon] sort up or ![icon] sort down to sort in ascending or descending order.

   • Click ![icon] **Filters** to filter by the status.

     • **Available**: Approved requests that are ready to view or copy.

     • **Pending Approval**: Requests that are waiting for approval.

     • **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.

     • **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.

     • **Expired**: Requests for which the **Checkout Duration** has elapsed.

     • **Denied**: Requests denied by the approver.

   • Click ![icon] **Search** to see a list of searchable elements. Or enter search characters. For more information, see Search box.

   • If a denied or revoked request has been commented on by an approver, you can click the ![icon] button associated with the request to view the comment.

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

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

    - The name, account, and remaining time is displayed.

    - If your browser allows, click 📋 **Copy** to check out the password. This puts the password onto your clipboard, ready for you to use. Or, click 👁 **Show** to check out the password and view the password. A password displays on your screen for 20 seconds. The web client displays up to 10,000 characters before truncating the password, however the API allows any set password payload below 1MB. If the password changes while you have it checked out, and your current request is still valid, select either 📋 **Copy** or 👁 **Show** again to obtain the new password.

    - Select 🚫 **Hide** to conceal the information from view.

    - Once you are done working, click ✅ **Check-In Request** to complete the password check out process.

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

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

- **Pending** request: Select ⊖ **Cancel Request** to remove the request.

- **Revoked** request: Select **Resubmit** to request the password again.

- **Expired** request: Select ⊖ **Remove Request** to delete the request from the list.

- **Denied** request: Select **Resubmit** to request the password again.

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

Approving a password release request

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

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

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

Safeguard for Privileged Passwords can be configured to notify you of a password release request that requires your approval. For more information, see Configuring alerts on page 35.

To approve or deny a password release request

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

- View details by selecting a request then looking at the details display on the right of the page.

- Approve one or more request: Select the requests. Then, click **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.

- Deny one or more request: Select the requests. Then, click **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.

- Change the columns that display: Click and select the columns you want to see. You can select columns including:

    - **Action**: Displays **Approve only this request** and **Deny only this request**.

    - **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).

    - **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, or **Telnet**).

    - **Account**: Displays the managed account name.

    - **Ticket Number**: Displays the ticket number, if required.

    - **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).

- **Search**: For more information, see Search box on page 30.

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 35.

To review a completed password release request

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

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.

- Mark one or more request as reviewed: Select the requests. Do the following:

  - If no comment is needed, click ![icon] **Mark all the selected requests as reviewed**.

  - If a comment is needed, this icon will display as ![icon] **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.

- Change the columns that display: Click ![icon] **Select columns to display** then select the columns you want to see.

  - **Action**: Displays ![icon] **This request requires review comments** or ![icon] **Mark only this request as reviewed**.
  - **Requester**: Displays the user name of the requester.
  - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.
  - **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 30.

SSH key release request workflow

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

Typically, an SSH key release request follows this workflow.

1. **Request**: Users that are designated as an authorized user of an entitlement can request SSH keys for any account in the scope of that entitlement's policies.

2. **Approve**: Depending on policy configuration, approval can be automatic or require the consent of one or more users which provides closer control over system accounts.

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

Requesting an SSH key release

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending SSH key release workflow events, such as when an SSH key release request is pending, denied, or revoked, and so forth. For more information, see Configuring alerts on page 35.

To request an SSH key release

1. Click 🏠**Home** then ⬛**New Request** or open ⬛**My Requests** then click ➕ **New Request**.

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

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

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

   - **Asset**: The display name of the managed system.

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

   - **Access Type**: The type of access request appears in the **Access Type** column. If the type is a drop-down, you can click the drop-down then multiple access request types are available. Click the drop-down and select the access type, in this case, **SSH Key**.

   - **Account Description**: (When applicable) The description of the account.

   - **Asset Description**: (When applicable) The description of the asset.

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

4. Click **Next**.

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

a. **Emergency Access**: If the policy has emergency access enabled, select this option to gain immediate emergency access to this SSH key. When you use **Emergency Access**, the request requires no approval.

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

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

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

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

   • View the **Checkout Duration**.

   • If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy.

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

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

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

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

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

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

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

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

When the request has been approved, you can use the SSH key. For more information, see Taking action on an SSH key release request on page 43.

Taking action on an SSH key release request

The actions that can be taken on an SSH key release request depends on the state of the request and the client interface you are using.

To take action on an SSH key release request

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

   - Click 🔵 then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.

   - Click **Sort By** ▼ then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.

   - Click ⬆ sort up or ⬇ sort down to sort in ascending or descending order.

   - Click ▼ **Filters** to filter by the status.

     - **Available**: Approved requests that are ready to view or copy.

     - **Pending Approval**: Requests that are waiting for approval.

     - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.

     - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.

     - **Expired**: Requests for which the **Checkout Duration** has elapsed.

     - **Denied**: Requests denied by the approver.

   - Click 🔍 **Search** to see a list of searchable elements. Or enter search characters. For more information, see Search box.

   - If a denied or revoked request has been commented on by an approver, you can click the 💬 button associated with the request to view the comment.

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

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

     a. The name, account, and remaining time is displayed. Click on the tile to see additional information or use the ⬛**Fetch SSH Details** button.

     b. The **Format** displays and can be selected, if necessary. Formats include **OpenSSH**, **SSH2**, and **PuTTY**. The **Format** chosen is preselected as the default for the next access request.

     c. Click ⬇**Checkout SSH Key** to check out the SSH key. This puts the SSH key onto your clipboard, ready for you to use.

     d. Click ▶ **Start SSH Session** to launch the session.

     e. **Private Key**: You can click 🖫**Save** or ⬚**Copy**.

f. **Passphrase**: You can click 👁**Show** or ⧉**Copy** if **Passphrase Protect SSH Key** was selected on when creating an access request policy.

g. The following types of information may display based on the format you select.

- **SHA-1 Fingerprint**
- **MD5 Fingerprint**
- **Public Key**: You can click 💾**Save** or ⧉**Copy**.

  If the SSH key changes while you have it checked out, and your current request is still valid, you can select the following to obtain an new SSH key, as available: 💾**Save**, ⧉**Copy**, or 👁**Show**.

h. Once you are done working, click ✅ **Check-In Request** to complete the SSH key check out process.

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

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

- **Pending** request: Select ⊖ **Cancel Request** to remove the request.

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

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

- **Expired** request: Select ⊖ **Remove Request** to delete the request from the list.

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

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

Approving an SSH key release request

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

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

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

Safeguard for Privileged Passwords can be configured to notify you of an SSH key release request that requires your approval. For more information, see Configuring alerts on page 35.

To approve or deny an SSH key release request

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

- View details by selecting a request then looking at the details display on the right of the page.

- Approve one or more request: Select the requests. Then, click **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.

- Deny one or more request: Select the requests. Then, click **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.

- Change the columns that display: Click and select the columns you want to see. You can select columns including:

  - **Action**: Displays **Approve only this request** and **Deny only this request**.
  - **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).
  - **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.
  - **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 30.

Reviewing a completed SSH key release request

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

You can configure Safeguard for Privileged Passwords to notify you of an SSH key release request that requires your review. For more information, see Configuring alerts on page 35.

To review a completed SSH key release request

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

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.

- Mark one or more request as reviewed: Select the requests. Do the following:

    - If no comment is needed, click ![icon] **Mark all the selected requests as reviewed**.

    - If a comment is needed, this icon will display as ![icon] **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.

- Change the columns that display: Click ![icon] **Select columns to display** then select the columns you want to see.

    - **Action**: Displays ⚠ **This request requires review comments** or ![icon] **Mark only this request as reviewed**.
    - **Requester**: Displays the user name of the requester.
    - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, or **Telnet**).
    - **Account**: Displays the managed account name.
    - **Ticket Number**: Displays the ticket number, if required.
    - **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page .

Session request workflow

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

Typically a session request follows the workflow below:

1. **Request**: Users that are designated as an authorized user of an entitlement can request a session for any asset in the scope of that entitlement's policies.

2. **Approve**: Depending on how the Security Policy Administrator configured the policy, a session request will either require approval by one or more 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.

About sessions and recordings

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

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

Important notes

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

Requesting session access

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending access request workflow events, such as when a session request is pending, denied, or revoked, and so on. For more information, see Configuring alerts on page 35.

To request session access

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

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

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

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

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

   - **Asset**: The display name of the managed system.

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

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

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

   - **Access Type**: The type of access request appears in the **Access Type** column. If the type is a drop-down, multiple access request types are available. Select the hyperlink and select the access type.

   - **Account Description**: (When applicable) The description of the account.

   - **Asset Description**: (When applicable) The description of the asset.

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

3. Click **Next**.

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

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

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

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

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

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

- View the **Checkout Duration**.

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

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

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

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

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

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

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

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

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

When the request has been approved, you can use the password. For more information, see Taking action on a password release request on page 38.

If the session does not launch

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

- `Please try again. The linked sessions module state is currently down or may be in a locked state.` This message may mean one of the following:

  - SPP could not contact SPS. Try again so the request can be redirected to another managed host in the SPS cluster.

- The SPS configuration is locked. Try again because this condition is typically because the SPS administrator is making configuration changes to the SPS appliance at the same time that a new access request is being created or a session is being launched.

- `Missing the session connection policy.` or
  `The selected Access Request Policy cannot be used to initiate a session from SPP. The highest priority policy must be associated with a valid SPS connection policy.`
  Check the connection policy configuration. In the web client, go to **Security Policy Management** > **Entitlements** > (edit) > **Access Request Policies** to add a valid connection policy. Save the policy and recreate the access request.

Taking action on a session request

The actions a user authorized to request access to a privileged session can take depends on the state of the request and the client interface you are using.

To take action on a session request

1. From the web client, click **My Requests**.

2. Search to find what you need. For more information, see Search box on page 30.

3. Click **Filters** to filter by the status.

   - **All**: Requests in all states.

   - **Available**: Approved requests that are ready (that is, a session that can be launched).

   - **Pending Approval**: Requests that are waiting for approval.

   - **Approved**: Requests that have been approved, but the check out time has not arrived.

   - **Revoked**: Approved requests retracted by the approver.

     - The approver can revoke a request after it is available.

     - When a user with Security Policy Administrator permissions revokes a live session, the active session is closed.

   - **Expired**: Requests for which the **Checkout Duration** has elapsed.

   - **Denied**: Requests denied by the approver.

4. Depending on the type of request, additional information may be available by clicking the tile.

5. You can take the following actions on session requests, depending on the state.

   - Available request: If the password or SSH key changes while you have it checked out, and your current request is still valid, select either **Copy** or **Show** again to obtain the new password or SSH key, if enabled by your Administrator.

- For SSH and RDP accounts:
    - The ▶**Start RDP Session**/**Start SSH Session** options are available only if enabled by user preferences. Click to launch the SSH client or RDP connection. For more information, see Launching the SSH client or Launching an RDP session.
    - Click ✔ **Check-In** to complete the check out process once you have ended your session.
    - In addition, you can use the following buttons to view or copy information into the dialog that contains the credentials needed to launch the session.
        - Click 🗗 **Copy** to check out and copy the credential.
        - Click 🕒**Show** to check out the credential and view the credential.
- For telnet or TN3270/TN5250 over telnet accounts, the fields needed are based on the terminal service application in use:
    - For a terminal service application that uses an inband connection string (like telnet), click 🗗 **Copy** to copy the **Hostname Connection String** and check out the password or SSH key. Then, paste the information in the log in screen.
    - If the terminal service application requires more information for log in (for example, TN3270/TN5250 over telnet):
        - Click 🕒 **Show** to display values that may include **Vault Address** (the SPP address), a one-time **Token**, **Username**, **Asset**, and **Sessions Module** (the SPS address).
        - Click 🗗 **Copy** by any of the values to copy a single value. Or, you can click 🗗 **Copy** at the right of all values to copy the entire the connection string, if that is required by your terminal service application.
        - Paste the necessary information into your terminal service application.
    - Click ✅ **Check-In Request** to complete the password or SSH key check out process. This makes the session request available to reviewers.
    - Click ⊘**Hide** to conceal the information from view.
- **Approved**: Select ⊖ **Cancel Request** to remove the request. A session request changes from Approved to Available when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
- **Pending**: Click ⊖ **Cancel Request** to remove the request.

- **Revoked**:
  - Click **Resubmit** to request the password or SSH key again.
  - Click ⊖ **Remove Request** to delete the request from the list.
- **Expired**: Click ⊖ **Remove Request** to delete the request from the list.
- **Denied**:
  - Click **Resubmit** to request the password or SSH key again.
  - Click ⊖ **Remove Request** to delete the request from the list.

Approving a session request

Depending on how the Security Policy Administrator configured the policy, a sessions request will either require approval by one or more 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 35.

To approve or deny a session request

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

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click ✅ **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click ⊘ **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click ⬚ and select the columns you want to see. You can select columns including:
  - **Action**: Displays ✅ **Approve only this request** and ⊘ **Deny only this request**.
  - **Requester / Status**: Displays the user name and the status of the approval (for example, **Pending 1 approval**).
  - **Asset / Access Type**: Displays the name of the asset and the type of access (for example, **Password**, **SSH Key**, **RDP**, **SSH**, or **Telnet**).
  - **Account**: Displays the managed account name.
  - **Ticket Number**: Displays the ticket number, if required.

- **Requested For**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search**: For more information, see Search box on page 30.

Launching the SSH client

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

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

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Hostname Connection String) required to launch the SSH client.

2. Click the ▶ **Start SSH Session** button associated with the asset name. In the web client, a session will launch if you have an application registered (ssh:// for SSH protocol).

   NOTE: The ▶ **Start SSH Session** options are available only if enabled by user preferences.

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

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

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

Launching an RDP session

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

To launch a remote desktop connection

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

2. In the web client:

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

- If you have an application registered (`rdp://` for RDP sessions), you can click the ▶ **Start RDP Session** button associated with the asset name then click **Connect**. See KB 313918 for details on application registration. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.

- If you do not have an application registered, download the RDP launch file instead of using the ▶ **Start RDP Session** button. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.

Begin your RDP session and close the session

1. In the remote desktop session, run the commands or programs on the target host. If there is no activity in an open session for about 10 minutes, the session will be closed. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.

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

Configuring and launching a Remote Desktop Application session

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

To configure and launch a remote desktop application

1. Install and configure Safeguard for Privileged Sessions's RemoteApp launcher available starting with 6.12. For more information, see One Identity Safeguard for Privileged Sessions Administration Guide.

2. Publish the **OISGRemoteAppLauncher** application following Microsoft's instructions. All remote applications that will be launched using SPP/SPS need to be configured to launch with the OISGRemoteAppLauncher and include a command line which references the intended remote application. Take note of the **RemoteApp Program Name** and **Alias** since they will be needed when configuring the access request policy.

3. On **Asset Management** > **Assets**, you need the following assets:

   a. **Windows Server** asset: This asset will be used to connect with a Windows Application Server.

   b. **Other**/**Other Managed** asset: This asset (of either platform type) is used to connect with the remote application. It requires the following settings:

      - **Network Address**: None

      - **Authentication Type**: None

      - An account from the remote application added to the **Accounts** tab.

4. On **Security Policy Management** > **Entitlements**, you will need an entitlement containing a Remote Desktop Application access request policy.

5. Within Safeguard for Privileged Sessions, a channel policy needs to be modified or created to include the following attributes. This channel policy will also need to be referenced from an RDP connection policy. For more information, see One Identity Safeguard for Privileged Sessions Administration Guide.

   a. In **RDP Control** > **Connections**, set the **Channel policy** to **applications**.

   b. In **RDP Control** > **Channel Policies**, create the following:

      i. **Dynamic virtual channel**: No configured settings.

      ii. **Custom**: Add the following to **Permitted channels**:

         - `rail`
         - `rail_ri`
         - `rail_wi`

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

To launch a remote desktop application connection

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

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

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

Reviewing a session request

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

NOTE: You can configure Safeguard for Privileged Passwords to notify you of an access request that requires your review. For more information, see Configuring alerts on page 35.

Desktop Player User Guide

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

To review a completed sessions request

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

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.

- Mark one or more request as reviewed: Select the requests. Do the following:

    - If no comment is needed, click **Mark all the selected requests as reviewed**.

    - If a comment is needed, this icon will display as **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.

- Change the columns that display: Click **Select columns to display** then select the columns you want to see.

    - **Action**: Displays **This request requires review comments** or **Mark only this request as reviewed**.

    - **Requester**: Displays the user name of the requester.

    - **Access Type**: Displays the type of access (for example, **Password**, **SSH Key**, **RDP**, **RDP Application**, **SSH**, or **Telnet**).

    - **Account**: Displays the managed account name.

    - **Ticket Number**: Displays the ticket number, if required.

    - **Request For/Duration**: Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).

- **Search**: For more information, see Search box on page 30.

About us

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

Contacting us

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

Technical support resources

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

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

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