



Safeguard for Privileged Passwords 6.0.8 LTS

User Guide

Copyright 2020 One Identity LLC.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of One Identity LLC .

The information in this document is provided in connection with One Identity products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of One Identity LLC products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, ONE IDENTITY ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL ONE IDENTITY BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF ONE IDENTITY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. One Identity makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. One Identity does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.

Patents

One Identity is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

Legend

 **WARNING:** A WARNING icon highlights a potential risk of bodily injury or property damage, for which industry-standard safety precautions are advised. This icon is often associated with electrical hazards related to hardware.

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

Contents

Introduction	5
Introduction to Safeguard for Privileged Passwords	5
Overview of the entities	7
Key features	13
System requirements and versions	17
Desktop client system requirements	18
Web client system requirements	19
Web management console system requirements	20
Supported platforms	20
License: hardware, virtual, expiration	25
Long Term Support (LTS) and Feature Releases	26
Search box	28
Search by attribute	29
Using the web client	32
My Requests (web client)	32
Approvals (web client)	33
Reviews (web client)	34
Favorites (web client)	34
Settings, version, and desktop Windows client (web client)	35
Change password (web client)	36
FIDO2 keys (web client)	37
Log out (web client)	37
Getting started with the desktop client	38
Installing the desktop client	38
Starting the desktop client	40
Uninstalling the desktop client	41
Using the desktop client	42
Settings (desktop client)	42
User information and log out (desktop client)	44
Desktop client favorite request	46

Desktop client navigation pane	47
Home	48
Privileged access requests	51
Configuring alerts	52
Toast notifications	52
Email notifications	52
Password release request workflow	53
Requesting a password release	53
Taking action on a password release request	55
Approving a password release request	58
Reviewing a completed password release request	59
Session request workflow	60
About sessions and recordings	61
Requesting session access	62
Taking action on a session request	65
Approving a session request	69
Launching the SSH client	71
Launching an RDP session	72
Reviewing a session request	74
Replaying a session	75
About us	77
Contacting us	77
Technical support resources	77
Index	78

Introduction

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

Introduction to Safeguard for Privileged Passwords

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

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

Safeguard privileged management software suite

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

The Safeguard products' unique strengths are:

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

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

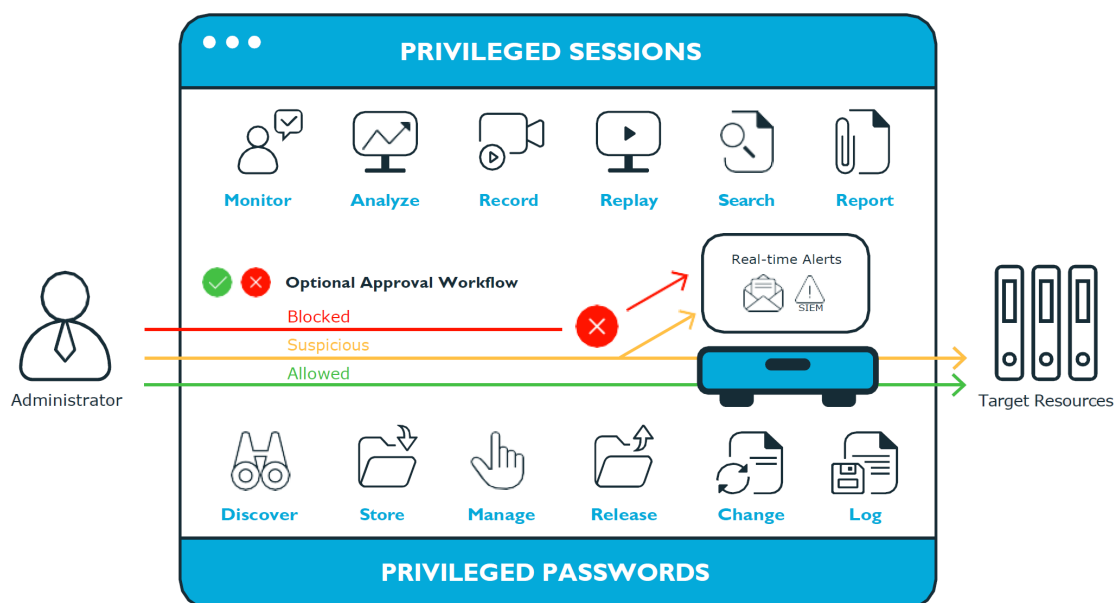
The suite includes the following modules:

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

Safeguard for Privileged Sessions is a quickly deployable enterprise appliance, completely independent from clients and servers to integrate seamlessly into existing networks. It captures the activity data necessary for user profiling and enables full user session drill-down for forensics investigations.

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

Figure 1: Privileged Sessions and Privileged Passwords



Overview of the entities

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

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

Assets, partitions, and partition profiles

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

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

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

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

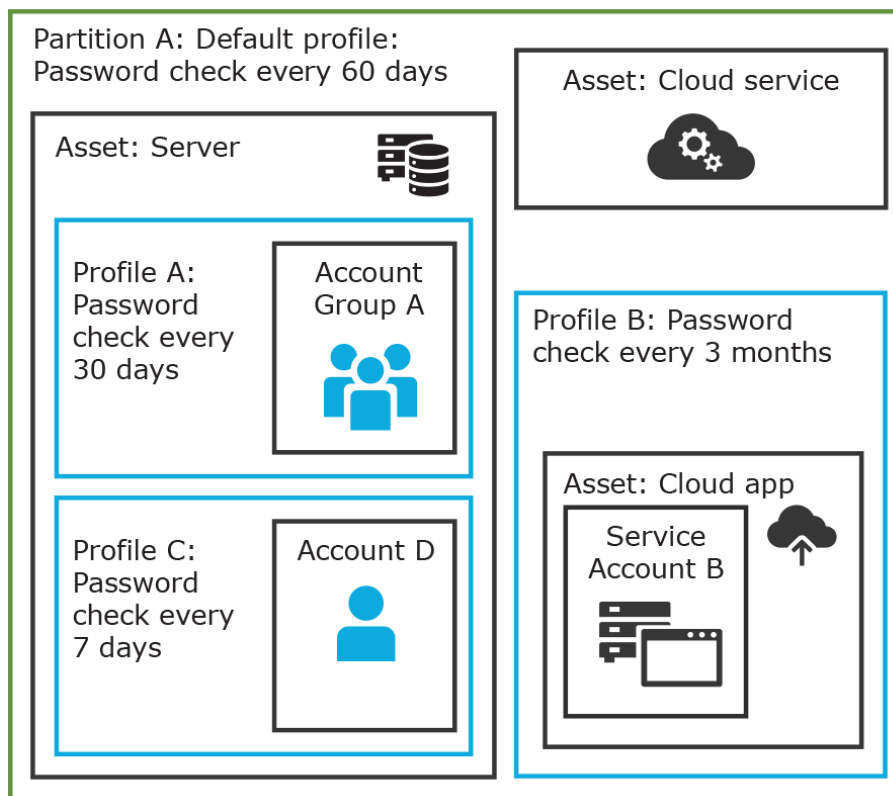
A partition can have multiple partition profiles, each assigned to different assets, if desired. An account is governed by only one profile. If an account is not explicitly assigned to a profile, the account is governed by the one assigned to the parent asset. If that asset does not have an assigned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

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

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

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

Figure 2: Password control



Details: Assets and asset groups

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

Details: Partitions and partition profiles

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

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

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

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

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

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

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

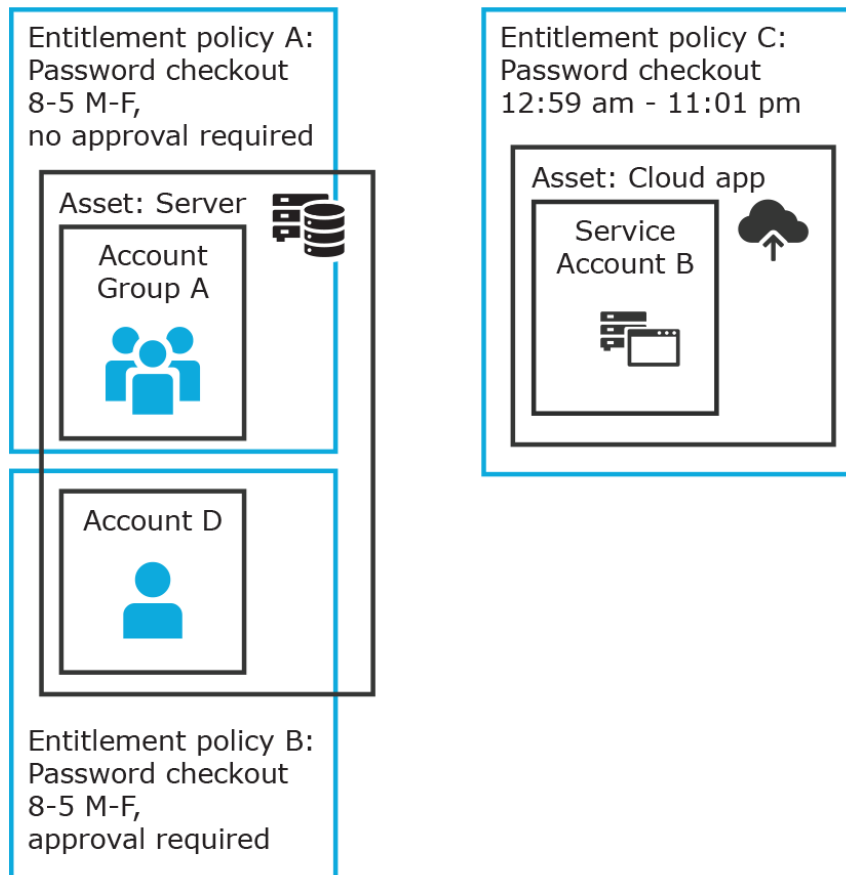
Entitlement access request policies may include:

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

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

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

Figure 3: Entitlements and accounts



Details: Accounts and account groups

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

Details: Entitlements and access request policies

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

Users and user groups

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

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

Users can be configured for two-factor authentication.

Details: Users and user groups

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

Discovery

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

Access request workflow

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

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

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

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

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

Key features

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

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

Table 1: One Identity Safeguard for Privileged Passwords key features

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

Feature	Description
Approval Anywhere	<p>This distributed clustering design also enables the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.</p>
Cloud support	<p>Safeguard for Privileged Passwordscan be run in the cloud using Azure or AWS.</p>
Directory integration	<p>You can leverage your existing directory infrastructure (such as Microsoft Active Directory). You import directory users and directory groups. Directory users authenticate to Safeguard for Privileged Passwords with their directory credentials. Managed account users cannot be members of the Protected Users AD Security Group.</p> <p>Active Directory and LDAP data is automatically synchronized by asset or identity and authentication providers schema as shown in the following lists.</p> <p>Asset schema list</p> <ul style="list-style-type: none"> • Users <ul style="list-style-type: none"> • Username • Password (modifiable in LDAP and not modifiable in Active Directory) • Description • Groups <ul style="list-style-type: none"> • Name • Member • Computer <ul style="list-style-type: none"> • Name • Network Address • Operating System • Operating System Version • Description <p>Identity and Authentication Providers schema list</p> <ul style="list-style-type: none"> • Users <ul style="list-style-type: none"> • Username • First Name

Feature	Description
	<ul style="list-style-type: none"> • Last Name • Work Phone • Mobile Phone • Email • Description • External Federation Authentication • Radius Authentication • Managed Objects • Groups <ul style="list-style-type: none"> • Name • Members • Description
Discovery	Quickly discover any privileged account or system on your network with host , directory, and network-discovery options.
Event notification options	Safeguard for Privileged Passwords allows you to configure the appliance to send event notifications to external systems such as Email, Syslog, and SNMP.
Favorites	Quickly access the passwords that you use the most right from the Home screen. You can group several password requests into a single favorite so you can get access to all the accounts you need with a single click.
One Identity Starling	Expand the capabilities of Safeguard with One Identity Starling, which offers immediate access to cloud delivered features and services. This includes all-you-can-eat Starling Two-Factor Authentication (2FA) to protect Safeguard access.
Partitions and Profiles	Safeguard for Privileged Passwords allows you to group managed systems into secure work areas that can be designated for delegated management.
Release control	Manages password requests from authorized users for the accounts they are entitled to access via a secure web browser connection with support for mobile devices.
RESTful API	Safeguard for Privileged Passwords (SPP) is built with an API-first design and uses a modernized API based on a REST architecture that allows other applications and systems. Every function is exposed through the API to enable quick and easy integration regardless of what you want to do or which language your applications are written in. There are even a few things that can

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

Sessions key features

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

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

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

System requirements and versions

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

- The Windows desktop client consists of an end-user view and administrator view. The fully featured desktop client exposes all of the functionality of Safeguard based on the role of the authenticated user.
- The web client is functionally similar to the desktop client end-user view and useful for requestors, reviewers, and approvers. Many administration functions are available as well.
- The web management console displays whenever you connect to the virtual appliance and is used for first time configuration. When setting up a virtual environment, carefully consider the configuration aspects such as CPU, memory availability, I/O subsystem, and network infrastructure to ensure the virtual layer has the necessary resources available. See [One Identity's Product Support Policies](#) for more information on environment virtualization.

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

If a Safeguard Sessions Appliance is joined to Safeguard for Privileged Passwords, session recording is handled via Safeguard for Privileged Session. The join is initiated from Safeguard for Privileged Sessions. For details about the join steps and issue resolution, see the [One Identity Safeguard for Privileged Sessions Administration Guide](#).

Bandwidth

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

Desktop client system requirements

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

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

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

If PuTTY is not found, the desktop client uses the version of PuTTY that it installed at:
<user-home-dir>/AppData/Local/Safeguard/putty.

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

Table 2: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6 (or later)
Windows platforms	64-bit editions of: <ul style="list-style-type: none">• Windows 7• Windows 8.1• Windows 10• Windows Server 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016 <p>If the appliance setting, TLS 1.2 Only is enabled, (Administrative Tools Settings Appliance Appliance Information), ensure the desktop client also has TLS 1.2 enabled. If the client has an earlier version of TLS enabled, you will be locked out of the client and will not be able to connect to Safeguard for Privileged Passwords.</p> <p>IMPORTANT: The Windows 7 Desktop client has additional requirements in order to enable TLS 1.2. For information, see</p>

Component	Requirements
	<p>Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows.</p> <p>Considerations:</p> <ul style="list-style-type: none"> Internet Explorer security must be set to use TLS 1.0 or higher. Ensure the proper "Use TLS" setting is enabled on the Advanced tab of the Internet Options dialog (In Internet Explorer, go to Tools Internet Options Advanced tab). To use FIDO2 two-factor authentication, you will need a web browser that supports the WebAuthn standard.
Desktop Player	See <i>One Identity Safeguard for Privileged Sessions [version] Safeguard Desktop Player User Guide</i> available at: One Identity Safeguard for Privileged Sessions - Technical Documentation, User Guide .

Web client system requirements

Table 3: Web requirements

Component	Requirements
Web browsers	<p>Desktop browsers:</p> <ul style="list-style-type: none"> Apple Safari 13.1 for desktop (or later) Google Chrome 80 (or later) Microsoft Edge 80 (or later) Mozilla Firefox 69 (or later) Microsoft Internet Explorer 11 (Newer features may not work with Internet Explorer. You are encouraged to upgrade to a browser that can support all functionality.) <p>Mobile device browsers:</p> <ul style="list-style-type: none"> Apple iOS 13 (or later) Google Chrome on Android version 80 (or later)

Web management console system requirements

Table 4: Web kiosk requirements

Component	Requirements
Web management console	<p>Desktop browsers:</p> <ul style="list-style-type: none">• Apple Safari 13.1 for desktop (or later)• Google Chrome 80 (or later)• Microsoft Edge 80 (or later)• Mozilla Firefox 69 (or later)• Microsoft Internet Explorer 11 (Newer features may not work with Internet Explorer. You are encouraged to upgrade to a browser that can support all functionality.)

Platforms and versions follow.

- You must license the VM with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative.
- Supported hypervisors:
 - Microsoft Hyper-V (VHDX) version 8 or higher
 - VMware vSphere with vSphere Hypervisor (ESXi) version 6.5 or higher
 - VMware Workstation version 13 or higher
- Minimum resources: 4 CPUs, 10GB RAM, and a 500GB disk. The virtual appliances default deploy does not provide adequate resources. Ensure these minimum resources are met.

Supported platforms

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

Safeguard for Privileged Passwords tested platforms

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

Other, **Other Managed**, or **Other Linux** selection on the **Management** tab of the **Asset** dialog.

SPP joined to SPS: Sessions platforms

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

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

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

Supported platform updates

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

Table 5: Supported platforms: Assets that can be managed

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

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

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

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

Table 6: Supported platforms: Directories that can be searched

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

For all supported platforms, it is assumed 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*.

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

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

- Command-Reference:
<https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/Command-Reference>
- Writing a custom platform script:
<https://github.com/OneIdentity/SafeguardCustomPlatform/wiki/WritingACustomPlatformScript>
- Example platform scripts are available at this location:
<https://github.com/OneIdentity/SafeguardCustomPlatform/tree/master/SampleScripts>

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

License: hardware, virtual, expiration

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

Hardware appliance

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

- Privileged Passwords

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

- If a Privileged Passwords module license is not installed, you will not be able to request a password release.

Virtual appliance licensing

You must license the virtual appliance with a Microsoft Windows license. We recommend using either the MAK or KMS method. Specific questions about licensing should be directed to your Sales Representative.

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

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

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

Long Term Support (LTS) and Feature Releases

Releases use the following version designations:

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

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

Table 7: Comparison of Long Term Support (LTS) Release and Feature Release

	Long Term Support (LTS) Release	Feature Release
Release frequency	<p>Frequency: Typically, every 2 years</p> <p>Scope: Includes new features, resolved issues and security updates</p> <p>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).</p>	<p>Frequency: Typically, every 3 months</p> <p>Scope: Includes the latest features, resolved issues, and other updates, such as security patches for the OS</p> <p>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).</p>

Maintenance Release	<p>Frequency: Typically, every 3 months during full support</p> <p>Scope: Includes critical resolved issues</p> <p>Versioning: A third digit designates the maintenance LTS Release (for example, 6.0.6 LTS).</p>	<p>Frequency: Only for highly critical issues</p> <p>Scope: Includes highly critical resolved issues</p> <p>Versioning: A third digit designates the maintenance Feature Release (for example, 6.6.1).</p>
Support	Typically 3 years after the original publication date or until the next LTS is published (whichever date is later)	Typically 6 months after the original publication date or until the next feature or LTS Release is published (whichever date is later)

Release details can be found at [Product Life Cycle](#).

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

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

Moving between LTS and Feature Release versions

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

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

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

Patching

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

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

Search box

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

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

Rules for using the search functionality:

- Search strings are not case-sensitive. Exception: in the web client, the Approvals and Reviews searches are case sensitive.
- Wild cards are not allowed.
- Try using quotes and omitting quotes. As you use the product, you will become familiar with the search requirements for the search fields you frequent. Safeguard may perform a general search (for example, omits quotes) or a literal search (for example, includes quotes). Example scenarios follow:
 - On the Settings pane, search strings must be an exact match because a literal search is performed. Do not add quotes or underlines. For example, from the Settings pane, enter password rules to return **Safeguard Access | Password Rules**. If you enter "**password rules**" or **password_rules**, the following message is returned: No matches found.
 - On the Users pane search box:
 - A general search does not return anything if you use quotes because it uses a literal search (searches for the quotes). For example: searching for "ab_misc2" returns the message: There is nothing to show here.
 - You can use quotes in an attribute search if there are spaces in the search name. For example, entering the following in the search box **Username: "ab_misc2"** returns: AB_misc2.
- When multiple search strings are included, all search criteria must be met in order for an object to be included in the results list.

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

To search for accounts

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

Examples:

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

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

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

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

You can also [Search by attribute](#).

Search by attribute

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

API attributes can be searched

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

Entering the search string

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

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

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

You can specify multiple attributes, repeating these steps to add an additional attribute to the search box. Do not add punctuation marks, such as commas or

colons, to separate the different attributes. When multiple attributes are included, all search criteria must be met in order for an object to be included in the results list.


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

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

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

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

Attributes in each Search box

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

Accounts

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

Account Groups

- Name
- Description
- Dynamic

Assets

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

Asset Groups

- Name
- Description

- Dynamic

Entitlements

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

Partitions

- Name
- Description

Users

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

User Groups

- Name
- Description


Using the web client






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


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

 (web client)

 (desktop client)

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

The pages available to you display on the left. You will see  **Home** and, based on your role, you may also see  **My Requests**,  **Approvals**,  **Reviews**,  **Settings**, or a combination of those. You can customize the information you see on the pages. For more information, see [Settings, version, and desktop Windows client \(web client\)](#) on page 35.


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

My Requests (web client)

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

To make a request


You must be an authorized user of an entitlement to create a request for the assets and accounts you need.






1. Click  **My Requests** to go to the **My Request** page.
2. Follow the workflow steps. For more information, see [Requesting a password release](#) on page 53.

To create a favorite

You can create favorites for requests you make often. For more information, see [Favorites \(web client\)](#) on page 34.


To view and manage requests



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

- Click **Sort By**  then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.
- Click  sort up or  sort down to sort in ascending or descending order.
- Click  **Filters** to filter by the status.
 - **All**: Requests in all states.
 - **Available**: Approved requests that are ready to view or copy.
 - **Pending Approval**: Requests that are waiting for approval.
 - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
 - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.
 - **Expired**: Requests for which the **Checkout Duration** has elapsed.
 - **Denied**: Requests denied by the approver.
- Click  **Search** to see a list of search-able elements. Or enter search characters. For more information, see [Search box](#).

Approvals (web client)


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



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

- Deny one or more request: Select the requests. Then, click  to deny all the selected requests. Optionally, enter a comment.
- Change the columns that display: Click  and select the columns you want to see.
- Search: For more information, see [Search box](#) on page 28.



For more information, see [Approving a password release request](#) on page 58.



Reviews (web client)

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



- View details: Select the request and the details display on the right of the page.
- Mark one or more request as reviewed: Select the requests. Then, click  **Mark all the selected requests as reviewed**. A comment may be required or, if not required, added.
- Change the columns that display: Click  **Select columns to display** then select the columns you want to see.
- Search: For more information, see [Search box](#) on page 28.

Favorites (web client)

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

You must be authorized to create requests for the assets and accounts you choose to include in a favorite. To change the look of the favorite tiles, click  for large icons or  for small icons.


Add a favorite

1. To the right of **My Favorite Requests**, click  **New Favorite**.
2. On the **Asset Selection** page, select the assets to access. Use the following approaches to quickly find the assets you want:
 - Click  **Search** to search the **Asset**, **Network Address**, or **Platform**. For more information, see [Search box](#) on page 28.

- Once you've selected assets, the number of **Assets selected** displays in the lower left. You can toggle between **Show only selected** and **Show all**.
 - In the lower right, select the number of **Items per page** that display. Click the arrows to move through the pages.
3. Click **Next**.
 4. On the **Account & Access Type Selection** page, select the account for the asset. If there are several accounts associated with an asset:
 - a. Click the **Select Account(s)** link.
 - b. Select the account(s) for that asset.
 - c. Click **OK**.
 - d. Continue to select accounts for each asset.
 5. Click **Next** to provide favorite details:
 - a. Enter a **Name** for the favorite.
 - b. Enter a **Brief Description**.
 - c. Select the color of the favorite's tile.
 6. Click **Add**.




Use and manage a favorite

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

1. Click the  menu on the right of the favorite and perform a task:
 - Click **Submit Request** to submit the request and launch the request workflow. Follow the workflow steps. For more information, see [Requesting a password release](#) on page 53.
 - Click **Change Color** to change the color of the favorite. This is useful to color code types of requests.
 - Click **Remove** to delete the favorite.

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

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




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

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

Change password (web client)






You can change your password.

To change the password

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

FIDO2 keys (web client)

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


1. In the upper right corner, next to your user name, click .
2. Click **Manage FIDO2 Keys**. The name and date each existing key was registered and last used displays.
3. Perform an action:
 - To change a name, enter the new name, then click  **Save**.
 - To remove a key, click  **Remove** by the key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.
 - To add a key, click  **Register New FIDO2 Key**.
 - a. You will be asked to insert or connect to the new key.
 - b. You will be prompted to reenter your primary credentials for verification.
 - c. Tap or activate your new FIDO2 key that is being registered.
 - d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name, then click  **Save**.

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

Log out (web client)

Always securely log out of the web client.

To log out

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

Getting started with the desktop client

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

Or, you can use the web client instead of the desktop client, if you Administrator has provided the url location. For more information, see [Using the web client](#) on page 32.

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

[Installing the desktop client](#)

[Starting the desktop client](#)

[Uninstalling the desktop client](#)

Installing the desktop client

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

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

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

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

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

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

Installing the Safeguard for Privileged Passwords desktop client application

1. To download the Safeguard for Privileged Passwords desktop client Windows installer .msi file, open a browser and navigate to:
`https://<Appliance IP>/Safeguard.msi`
Save the **Safeguard.msi** file in a location of your choice.
2. Run the MSI package.
3. Select **Next** in the **Welcome** dialog.
4. Accept the **End-User License Agreement** and select **Next**.
5. Select **Install** to begin the installation.
6. Select **Finish** to exit the desktop client setup wizard.
7. Check your desktop resolution. The desktop client works the best at a resolution of 1024 x 768 or greater.

Installing the Desktop Player

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

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

New Desktop Player versions

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

Starting the desktop client

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

To start the desktop client application

1. From the Windows Start menu, choose **Safeguard**.
2. On the server selection screen, enter or select the server's network DNS name or IP address to connect to the appliance over the network and click **Connect**.
NOTE: When entering an IPv6 address, enclose the IPv6 address in square brackets.
3. You will see a message like: You'll now be redirected to your web browser to complete the login process. You can select: Don't show this message again. Then, click **OK**.
4. On the user login screen, enter your credentials and click **Log in**.
 - User Name: Enter your user or display name. Do not include spaces in the User Name.
NOTE: When using directory account credentials, you have the option to enter your domain\name.
 - Password: Enter the password associated with the user entered above.
5. If your Safeguard for Privileged Passwords user account requires you to log in with secondary authentication, enter the secure password token code, or other authentication for your authentication service provider account and click **Submit**.
NOTE: The type and configuration of the secondary authentication provider (for example, RSA SecureID, FIDO2, One Identity Starling Two-Factor Authentication, and so on) determines what you must provide for secondary authentication. Check with your system administrator for more information about how to log in to Safeguard for Privileged Passwords with secondary authentication.
6. When login is successful, you can close the web browser and return to the Safeguard application.

To remove server DSN names or IP addresses no longer used

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

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


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

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

Uninstalling the desktop client

You can uninstall a desktop client.

To uninstall the desktop client

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

Using the desktop client

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

- Windows desktop client: The desktop client consists of an end-user view and an administrator view. The administrative functionality is dynamically enabled based on the user's permissions. The desktop client user interface information follows.
- Web client: The web client is functionally similar to the desktop client end-user view. For more information, see [Using the web client](#) on page 32.

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





(web client)



(desktop client)

Desktop client toolbar

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

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

Settings (desktop client)

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

Notifications

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

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

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

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

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

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

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

Widgets

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

- Requests
- Approvals
- Reviews


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

About dialog tab

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

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

User information and log out (desktop client)



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

My Account


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

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

To update your personal information





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


To change your user password

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

To manage your FIDO2 keys


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

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

- Click  **Delete** to delete a key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.
 - Click **Register New FIDO2 Key** to add a key.
 - a. You will be asked to insert or connect to the new key.
 - b. You will be prompted to reenter your primary credentials for verification.
 - c. Tap or activate your new FIDO2 key that is being registered.
 - d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name.
3. Click **Done** to close the My Accounts pane.

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

To manage the notifications you receive

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

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

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

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

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

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

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

Log Out

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

Desktop client favorite request

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

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

To create a favorite request from your Home page

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

Click **Add**.

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

To create a favorite request from the New Access Request dialog

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

- a. **Name:** Enter a name for the request.
 - b. **Description:** Enter descriptive text about the request.
 - c. **Color:** Select the icon color to be used to display the request in your Favorites list.
3. Click **Add**.

To change a favorite request's icon color





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


To remove a favorite request

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


Desktop client navigation pane

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

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


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

Home

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

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

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

- Customize the information that is displayed on each page. Click  **Dashboard settings**. For more information, see [Settings, version, and desktop Windows client \(web client\)](#) on page 35.
- Read the **Message of the Day** from the Appliance Administrator.
- Create favorites for requests you make often. For more information, see [Favorites \(web client\)](#) on page 34.

Requester's Home page view

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

For more information, see:

- [Requesting a password release](#)
- [Requesting session access](#)

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

For more information, see:

- [Taking action on a password release request](#)
- [Taking action on a session request](#)

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

Favorites pane: Action bar buttons

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

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

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

Submit a favorite request

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

For more information, see:

- [Desktop client favorite request](#)

Approver's Home page view

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

For more information, refer to these topics:

- [Approving a password release request](#)
- [Approving a session request](#)

Reviewer's Home page view

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

For more information, refer to these topics:

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

Privileged access requests

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



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

As a Safeguard for Privileged Passwords user, your **Home** page provides a quick view to the access request tasks that need your immediate attention. In addition, an Administrator can set up alerts to be sent to users when there are pending tasks needing attention. For more information, see [Configuring alerts](#) on page 52.

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

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

Requesters can also define favorite requests, which then appear on their **Home** page for subsequent use. This can be done from either the desktop client or web client:

-  Desktop client: For more information, see [Desktop client favorite request](#) on page 46.
-  Web client: For more information, see [Favorites \(web client\)](#) on page 34.
- Approvers see tasks related to approving (or denying) and revoking access requests.
- Designated reviewers see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

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

- [Password release request workflow](#)
- [Session request workflow](#)

Configuring alerts

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

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


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

Toast notifications

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



(desktop client) To enable toast notifications

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

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

Email notifications

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

- For Local users, you must set your email address correctly in the desktop client, **My Account**. For more information, see [User information and log out \(desktop client\)](#) on page 44.
- 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

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

Typically, a password release request follows this workflow.

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

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



Requesting a password release

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

You can configure Safeguard for Privileged Passwords to notify you of pending password release workflow events, such as when a password release request is pending, denied, or revoked, and so forth. For more information, see [Configuring alerts](#) on page 52.

To request a password release

1. Go to the new access request page:

-  (web client): Click **Home** or **My Requests**, then click **+ New Request**.
-  (desktop client): Go to the **Home** page, then click **New Request**.

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

2. On **Asset Selection**, select the assets to be included in the access request. The assets available for selection are based on the scope defined in the entitlement's access request policies. There is a limit of 50 assets.
3. On **Account & Access Type Selection**, select the accounts to be included in the access request and the type of access being requested for each selected account. The accounts include linked accounts, if any.
 - **Asset:** The display name of the managed system.
 - **Account:** The available account appears in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.
 - **Access Type:** The type of access request appears in the **Access Type** column. If the type is a hyperlink, multiple access request types are available. Select the hyperlink and select the access type.

You can remove an asset or account from the list. Select the entry in the grid and click **-Delete**.

4. On **Request Details**, configure the following settings, which will apply to all of the selected assets and accounts:
 - a. **Normal Access:** If the policy has emergency access enabled, select this option to gain normal access to this password. Normal access ensures the access request goes through the entire end-to-end access release process from request to approval to review as defined in the policy by the Security Policy Administrator.
 - b. **Emergency Access:** If the policy has emergency access enabled, select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval.
 - c. **Request Immediately:** If selected, the request is immediately created. You can clear this option to enter a specific date and time for the request in the user's local time.
 - d. **Checkout Duration:** Based on the policy, do one of the following:
 - View the **Checkout Duration**.
 - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy.
 - e. **Ticket Number:** If the policy requires a ticket number, enter a ticket number.

If multiple accounts are in the request and one or more require a ticket number, the ticket number is applied to all of the requests associated with this access request. This feature is set up through the desktop client.

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



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

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

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

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

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

- In the web client, favorites are displayed on the  **Home** page and the  **My Requests** page. For more information, see [Favorites \(web client\)](#) on page 34.
- In the desktop client, select the favorite request from the **Favorites** pane. In the **New Access Request** dialog, you can edit the request details or enter a required reason or comment before submitting the request. For more information, see [Desktop client favorite request](#) on page 46.

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



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
















When the request has been approved, you can use the password. For more information, see [Taking action on a password release request](#) on page 55.




Taking action on a password release request

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




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








1. From the web client, click  **My Requests**. Use any of the following methods to control the request displayed:
 - Click **Sort By**  then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.








- Click  sort up or  sort down to sort in ascending or descending order.
 - Click  **Filters** to filter by the status.
 - **All**: Requests in all states.
 - **Available**: Approved requests that are ready to view or copy.
 - **Pending Approval**: Requests that are waiting for approval.
 - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
 - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.
 - **Expired**: Requests for which the **Checkout Duration** has elapsed.
 - **Denied**: Requests denied by the approver.
 - Click  **Search** to see a list of search-able elements. Or enter search characters. For more information, see [Search box](#).
2. You can take any of the following actions on the password release request:
- **Available** request: Make selections on the request based on your user interface.
 - Click on  to expand the box to see the options.
 - If your browser allows, click  **Copy** to check out the password. This puts the password into your copy buffer, ready for you to use. Or, click  **Show** to check out the password and view the password. A password displays on your screen for 20 seconds. If the password changes while you have it checked out, and your current request is still valid, select either  **Copy** or  **Show** again to obtain the new password.
 - Select  **Hide** to conceal the information from view.
 - Once you are done working, click  **Check-In** to complete the password check out process.
 - **Approved** request: Select  **Cancel** to remove the request.
A password release request changes from **Approved** to **Available** when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
 - **Pending** request: Select  **Cancel** to remove the request.
 - **Revoked** request: Select  **Resubmit Request** to request the password again.
Select  **Remove** to delete the request from the list.

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

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

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

NOTE: You enable or disable the **Home** page widgets in the  [Settings \(desktop client\)](#) menu.
2. Open the list of requests and select one of the following view filters. The number indicates how many requests are in that state.
 - **All:** Requests in all states.
 - **Available:** Approved requests that are ready to view or copy.
 - **Approved:** Requests that have been approved, but the check out time has not arrived.
 - **Pending:** Requests that are waiting for approval or for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
 - **Revoked:** Approved requests retracted by the approver. The approver can revoke a request between the time the requester views the password and checks it in.
 - **Expired:** Requests for which the **Checkout Duration** has elapsed.
 - **Denied:** Requests denied by the approver.
3. Select an account to see the details of the password release request.
4. Take the following actions on password release requests:
 - **Available:** Make selections on the request based on your user interface.
 - Click  **Copy** to check out the password. This puts the password into your copy buffer, ready for you to use. Or, click  **Show** to check out the password and view the password. A password displays on your screen for 20 seconds. If the password changes while you have it checked out, and your current request is still valid, select either  **Copy** or  **Show** again to obtain the new password.
 - Select  **Hide** to conceal the information from view.
 - Once you are done working, click  **Check-In** to complete the password check out process.

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

Approving a password release request


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




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

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




Safeguard for Privileged Passwords can be configured to notify you of a password release request that requires your approval. For more information, see [Configuring alerts](#) on page 52.

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

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




- View details: Select the request and the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click  to approve all the selected requests. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click  to deny all the selected requests. Optionally, enter a comment.
- Change the columns that display: Click  and select the columns you want to see.
- Search: For more information, see [Search box](#) on page 28.

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

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

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

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

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



Reviewing a completed password release request

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




You can configure Safeguard for Privileged Passwords to notify you of a password release request that requires your review. For more information, see [Configuring alerts](#) on page 52.

(web client) To review a completed password release request



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

- View details: Select the request and the details display on the right of the page.
- Mark one or more request as reviewed: Select the requests. Then, click  **Mark all the selected requests as reviewed**. A comment may be required or, if not required, added.
- Change the columns that display: Click  **Select columns to display** then select the columns you want to see.
- Search: For more information, see [Search box](#) on page 28.

(desktop client) To review a completed password release request

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

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

2. Open the list of pending reviews and select an account name to see the details of the password release request.
3. Take the following action on password release requests:
 - Select  **Workflow** to review the transactions that took place in the selected request.
 - Select  **Review** to complete the review process.
Optionally, enter a comment of up to 255 characters.

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

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

Session request workflow

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

Typically a session request follows the workflow below:

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

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

About sessions and recordings

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

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

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

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

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

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

Important notes

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

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

- All session activity (every packet sent and action that takes place on the screen, including mouse movements, clicks, and keystrokes) is recorded and available for play back.
- If Safeguard for Privileged Passwords detects no activity for 10 minutes during a privileged session, the session is terminated.

Requesting session access

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

You can configure Safeguard for Privileged Passwords to notify you of pending access request workflow events, such as when a session request is pending, denied, or revoked, and so on. For more information, see [Configuring alerts](#) on page 52.

To request session access

1. Go to the new access request page:

- From the web client, click **Home** or **My Requests**, then click **+ New Request**.
- From the desktop client, go to the **Home** page, then click **New Request**.

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

2. On **Asset Selection**, select the assets to be included in the access request. The assets available for selection are based on the scope defined in the entitlement's access request policies. The limit is 50 assets.
If an SPS_Initiated connection policy is selected when creating an access request, the assets associated by that request will not display. The session-related access policy assigned to SPS_Initiated is filtered out. A connection policy other than SPS_Initiated must be selected to create an Access Request for the asset.
3. On **Account & Access Type Selection**, select the accounts to be included in the access request and the type of access being requested for each selected account. The accounts include linked accounts, if any.
- **Asset:** The display name of the managed system.
 - **Network Address:** The network host name or IP address of the managed system.
 - **Account:** The accounts available appear in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.

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






The settings are:





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

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

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

4. On the **Request Details** tab, configure the following settings, which will apply to all of the selected assets and accounts:
 - a. **Normal Access:** If the policy has emergency access enabled, select this option to gain normal access to this password. Normal access ensures the access request goes through the entire end-to-end access release process from request to approval to review as defined in the policy by the Security Policy Administrator.
 - b. **Emergency Access:** If the policy has emergency access enabled, select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval.
 - c. **Request Immediately:** Clear this option to enter a specific date and time for the request. Enter the time in the user's local time.

- d. **Checkout Duration:** This either displays the **Checkout Duration**; or, if the **Allow Requester to Change Duration** option is enabled in the policy, it allows you to set the days, hours, and minutes that you want the password and overrides the **Checkout Duration** set in the access request policy.
 - e. **Ticket Number:** If the policy requires a ticket number, enter a valid ticket number for this request. When multiple accounts are specified in the request, if any of the selected accounts require a ticket number, you must specify a valid ticket number. The specified ticket number will be applied to all of the requests associated with this access request. This feature is set up through the desktop client.
 - f. **Reason:** If the policy requires reason, select an access request reason code for this request. Select the **Description** down arrow to view the description defined for the selected reason. When multiple accounts are specified in the request, if any of the selected accounts require a reason, you must specify a reason. The specified reason will be applied to all of the requests associated with this access request.
 - g. **Comment:** Enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 255 characters.
5. To save the access request as a favorite, click the **Add to Favorites** button.
- Add to Favorites** displays, allowing you to specify a name and description for the access request. It also allows you to assign a color to the request's icon.
- This access request is then added to your **Favorites**. How you manage favorites depends on your interface:
- In the web client, favorites are displayed on the  **Home** page and the  **My Requests** page. For more information, see [Favorites \(web client\)](#) on page 34.
 - In the desktop client, select the favorite request from the **Favorites** pane. In the **New Access Request** dialog, you can edit the request details or enter a required reason or comment before submitting the request. For more information, see [Desktop client favorite request](#) on page 46.
6. After entering the required information, click **Submit Request**. **Access Request Result** displays showing you the access requests submitted and whether a request was successful.
7. To copy or view information, click the  (**expand down**) arrow on the left of an active request.
- If the access request is for sessions:
 - Click  **Copy** to copy the connection string to the clipboard. Paste the string into a client application to launch the session.
 - Click  **Show** to view the connection string.

- Click  **Help** to copy the value into the appropriate field of the configuration dialog.
- If the access request is for passwords:
 - Click  **Copy** to copy credential to the clipboard. The credential can then be pasted into the dialog that needs the credential to grant access.
 - Click  **Show** to view the credential.
 - Click  **Help** to copy the value into the appropriate field of the configuration dialog.

If the session does not launch


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











- Please try again. The linked sessions module state is currently down or may be in a locked state. This message may mean one of the following:
 - SPP could not contact SPS. Try again so the request can be redirected to another managed host in the SPS cluster.
 - The SPS configuration is locked. Try again because this condition is typically because the SPS administrator is making configuration changes to the SPS appliance at the same time that a new access request is being created or a session is being launched.
- Missing the session connection policy. or
The selected Access Request Policy cannot be used to initiate a session from SPP. The highest priority policy must be associated with a valid SPS connection policy.
Check the connection policy configuration. In the desktop client, go to **Entitlements | Access Request Policy | Sessions Settings** to add a valid connection policy. Save the policy and recreate the access request. For more information, see Session Settings tab in the *Safeguard for Privileged Passwords Administration Guide*.













Taking action on a session request

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





(web client) To take action on a session request









1. From the web client, click  **My Requests**.
2. Search to find what you need. For more information, see [Search box](#) on page 28.













3. Click  **Filters** to filter by the status.
 - **All:** Requests in all states.
 - **Available:** Approved requests that are ready (that is, a session that can be launched).
 - **Pending Approval:** Requests that are waiting for approval.
 - **Approved:** Requests that have been approved, but the check out time has not arrived.
 - **Revoked:** Approved requests retracted by the approver.
 - The approver can revoke a request after it is available.
 - When a user with Security Policy Administrator permissions revokes a live session, the active session is terminated.
 - **Expired:** Requests for which the **Checkout Duration** has elapsed.
 - **Denied:** Requests denied by the approver.
4. Click  or  to see more or less information on the request.
5. You can take the following actions on session requests, depending on the state.
 - **Available:** If the password changes while you have it checked out, and your current request is still valid, select either  **Copy** or  **Show** again to obtain the new password, if enabled by your Administrator. **Seconds Remaining** shows you how long you have to copy information to use to log in.
 - For SSH and RDP accounts:
 - Click  **Launch** to launch the SSH client or RDP connection. For more information, see [Launching the SSH client](#) or [Launching an RDP session](#).
 - Click  **Check-In** to complete the check out process once you have ended your session.
 - In addition, you can use the following buttons to view or copy information into the dialog that contains the credentials needed to launch the session.
 - Click  **Copy** to check out and copy the credential.
 - Click  **Show** to check out the credential and view the credential.
 - For telnet or TN3270/TN5250 over telnet accounts, the fields needed are based on the terminal service application in use:
 - For a terminal service application that uses an inband connection string (like telnet), click  **Copy** to copy the **Hostname Connection** string and check out the password. Then, paste the information in the log in screen.

- If the terminal service application requires more information for log in (for example, TN3270/TN5250 over telnet):
 - Click  **Show** to display values that may include **Vault Address** (the SPP address), a one-time **Token, Username, Asset,** and **Sessions Module** (the SPS address).
 - Click  **Copy** by any of the values to copy a single value. Or, you can click  **Copy** at the right of all values to copy the entire the connection string, if that is required by your terminal service application.
 - Paste the necessary information into your terminal service application.
- Click  **Check-In** to complete the password check out process. This makes the session request available to reviewers.
- Click  **Hide** to conceal the information from view.
- **Approved:** Select  **Cancel** to remove the request. A session request changes from Approved to Available when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
- **Pending:** Click  **Cancel** to remove the request.
- **Revoked:**
 - Click  **Resubmit Request** to request the password again.
 - Click  **Remove** to delete the request from the list.
- **Expired:** Click  **Remove** to delete the request from the list.
- **Denied:**
 - Click  **Resubmit Request** to request the password again.
 - Click  **Remove** to delete the request from the list.

(desktop client) *To take action on a session request*

1. From your  **Home** page, use any of these controls on the **Requests** widget, as needed. You can enable or disable the **Home** page widgets in the  **Settings** (desktop client) menu.
 - Select  (**expand down**) to open the list of active requests.
 - Select  **Popout**. You can then select and drag the pane to any location on the console and re-size the window to float the **Requests** pane.
2. Open the list of requests and select one of these view filters. The number indicates how many requests are in that state.
 - **All:** Requests in all states
 - **Available:** Approved requests that are ready (that is, a session that can be launched)

- **Approved:** Requests that have been approved, but the check out time has not arrived
 - **Pending Approval:** Requests that are waiting for approval
 - **Revoked:** Approved requests retracted by the approver
 - The approver can revoke a request between the time the requester launches the session and checks it back in.
 - When a user with Security Policy Administrator permissions revokes a live session, the active session is terminated.
 - **Expired:** Requests for which the **Checkout Duration** has elapsed.
 - **Denied:** Requests denied by the approver.
3. Select an account to see the details of the session request.
 4. You can take the following actions on session requests, depending on the state.
 - **Available:** If the password changes while you have it checked out, and your current request is still valid, select either  **Copy** or  **Show** again to obtain the new password, if enabled by your Administrator. **Seconds Remaining** shows you how long you have to copy information to use to log in.
 - For SSH and RDP accounts:
 - Click  **Launch** to launch the SSH client or RDP connection. For more information, see [Launching the SSH client](#) or [Launching an RDP session](#).
 - Click  **Check-In** to complete the check 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.
 - Click  **Help** to copy the value into the appropriate field of the configuration dialog.
 - For telnet or TN3270/TN5250 over telnet accounts, the fields needed are based on the terminal service application in use:
 - For a terminal service application that uses an inband connection string (like telnet), click  **Copy** to copy the **Hostname Connection** string and check out the password. Then, paste the information in the log in screen.
 - If the terminal service application requires more information for log in (for example, TN3270/TN5250 over telnet):

- Click  **Show** to display values that may include **Vault Address** (the SPP address), a one-time **Token, Username, Asset,** and **Sessions Module** (the SPS address).
- Click  **Copy** by any of the values to copy a single value. Or, you can click  **Copy** at the right of all values to copy the entire the connection string, if that is required by your terminal service application.
- Paste the necessary information into your terminal service application.
- Click  **Check-In** to complete the password check out process. This makes the session request available to reviewers.
- Click  **Hide** to conceal the information from view.
- **Approved:** Select  **Cancel** to remove the request. A session request changes from **Approved** to **Available** when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
- **Pending Approval:** Click  **Cancel** to remove the request.
- **Revoked:**
 - Click  **Resubmit Request** to request the password again.
 - Click  **Remove** to delete the request from the list.
- **Expired:** Click  **Remove** to delete the request from the list.
- **Denied:**
 - Click  **Resubmit Request** to request the password again.
 - Click  **Remove** to delete the request from the list.




Approving a session request

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




You can configure Safeguard for Privileged Passwords to notify you of an access request that requires your approval. For more information, see [Configuring alerts](#) on page 52.

(web client) To approve or deny a session request

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

- View details: Select the request and the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click  to approve all the selected requests. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click  to deny all the selected requests. Optionally, enter a comment.
- Change the columns that display: Click  and select the columns you want to see.
- Search: For more information, see [Search box](#) on page 28.

(desktop client) To approve or deny a sessions request

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




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

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

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

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

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

State	Actions
Pending	Select  to Approve or Deny a sessions request. Optionally, enter a comment of up to 255 characters.
Pending Additional Approvers	Select  to Deny a sessions request. Optionally, enter a comment of up to 255 characters.
Approved	Select  to Deny or Revoke an approved request.




State	Actions
	<p>You can revoke a request between the time the requester views it and checks it in.</p> <p>Any eligible approver can deny an access request after it has already been approved or auto-approved. Once disallowed, the requester will no longer be able to access the requested session, but they are given another opportunity to request that session again. The requester receives an email notifying them that the request was denied. For more information, see Configuring alerts on page 52.</p>

Launching the SSH client

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

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

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Hostname Connection String) required to launch the SSH client.
2. Click the ► **Launch** button to the right of the asset name.
 - In the web client, a session will launch if you have an application registered (ssh:// for SSH protocol).
 - In the desktop client, clicking ► **Launch** displays the **PuTTY Configuration** dialog. The required information is populated, click **Open** to launch the SSH client. If the required information is not populated in the **PuTTY Configuration** dialog, use the following buttons to copy and paste the information into the dialog:
 - Use the buttons to the right of the **Hostname Connection String** to perform the following tasks:
 - **View**: To view the hostname connection string
 - **Copy**: To copy the value to your copy buffer, which can then be pasted into the Hostname field of the **PuTTY Configuration** dialog
 - **Help**: To copy the value into the Hostname field of the PuTTY Configuration dialog
 - Use the buttons to the right of the **Password** to perform the following tasks.

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

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

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

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





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

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

Launching an RDP session

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

To launch a remote desktop connection

1. If the **User Supplied** option is selected in the policy, you will be prompted to enter your user credentials. After entering the requested credentials, click **Apply**. This will retrieve the information (for example, Username Connection String) required to launch the remote desktop session.
2. Depending on your interface:
 -  (desktop client) Click the  **Launch** button to the right of the asset name. Clicking this button displays the **Remote Desktop Connection** dialog. Click **Connect** to launch the remote desktop session.
 -  (web client) In the web client:
 - If you have an application registered (rdp:// for RDP sessions), you can click the  **Launch** button to the right of the asset name then click **Connect**. See [KB 313918](#) for details on application registration. A password must be entered and we recommend sg. A blank password will

cause the session to fail.

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

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

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

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

Begin your RDP session and close the session

1. In the remote desktop session, run the commands or programs on the target host. If there is no activity in an open session for about 10 minutes, the session will be terminated. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.
2. Once you are completed, log out of the target host and select ✓ **Check in** to complete the session request process.

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

Reviewing a session request


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



NOTE: You can configure Safeguard for Privileged Passwords to notify you of an access request that requires your review. For more information, see [Configuring alerts](#) on page 52.

Desktop Player User Guide




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

(web client) To review a completed sessions request

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



- View details: Select the request and the details display on the right of the page.
- Mark one or more request as reviewed: Select the requests. Then, click  **Mark all the selected requests as reviewed**. A comment may be required or, if not required, added.
- Change the columns that display: Click  **Select columns to display** then select the columns you want to see.
- Search: For more information, see [Search box](#) on page 28.

(desktop client) To review a completed sessions request

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

You can then select and drag the pane to any location on the console and resize the window.

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

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

A ● (green dot) indicates the session is live. A user with Security Policy Administrator permissions can click this icon to follow an active session. If the session recording has been archived from the local Safeguard file system or was recorded prior to joining a Sessions Appliance, you will see a **Download** button instead of a **Play** button. Click **Download** to download the recording and then click **Play**.

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

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

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

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

Optionally, enter a comment of up to 255 characters.

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

Replaying a session

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

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

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

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

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

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

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

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

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

3. Accept the certificate to continue.

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

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

Desktop Player User Guide

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

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.

A

- access request workflow 51
- approve password release request 58, 69
 - desktop client 59
- approve session access request 70

C

- configure alerts 52
- contact information
 - change personal information 44

D

- desktop client
 - application settings 42
 - install 38
 - start 40
 - system requirements 18
 - uninstall 41
- directories that can be searched 20
- disable
 - toast notifications 52

E

- email
 - configure Safeguard to receive notifications 52
- enable
 - toast notifications 43, 52

F

- favorites
 - create 46
 - remove 47
 - set color 47
- FIDO key 37, 44

H

- Home page
 - about 48
 - navigation pane 47

I

- install
 - desktop client 38

L

- launch
 - RDP session 72
 - Safeguard Desktop Player 75
 - SSH client 71
- licensing 25

P

- partition
 - about 7
- password
 - change 44

- password release
 - check-in 56-57
 - checkout 56-57
- password release request 53
 - cancel pending request 56, 58
 - desktop client approval 59
 - desktop client check-in 57
 - desktop client checkout 57
 - remove request 56, 58
 - resubmit request 57-58, 67, 69
 - review 59-60
 - web client approval 58, 69
 - web client check-in 55
 - web client checkout 55
 - workflow 53
- photo
 - change 44
- platforms that can be managed 20
- play back recorded session 75
- product licensing 25
- profile
 - about 7-8

R

- RDP session
 - launch 72
- replay recorded session 75
- request password release 53
- request workflow
 - dialog 75
 - password release requests 53
- review
 - password release request 59-60
 - session access request 74
 - session release request 74

- run in the system tray 43

S

- Safeguard
 - features 13
- search box 28
 - using 28-29
- secondary authentication
 - login 40
- session access request 62
 - approve 70
 - check-in session 65, 67
 - launch RDP session 72
 - launch session 65, 67
 - launch SSH client 71
 - review 74
 - revoke 70
- session recording
 - about 61
 - play back 75
- session release
 - checkout 66, 68
- session release request
 - cancel pending request 67, 69
 - remove request 67, 69
 - review 74
- session request workflow 60
- sessions
 - about 61
- settings
 - desktop client application settings 42
 - run in the system tray 43
- SSH session
 - launch SSH client 71
- start desktop client 40

- supported platforms 20
- system requirements 17
 - desktop client 18
 - web client 19
 - web management console 20

- web management console
 - system requirements 20
- widgets
 - approvals widget, controls 59, 70
 - requests widget, controls 67
 - reviews widget, controls 60, 74

T

- toast notifications 52
 - about 43
- toolbar
 - main screen 42

U

- uninstall desktop client 41
- user
 - change password 44
 - change personal contact information 44
 - change photo 44

W

- web client 32
 - about 42
 - approvals 33
 - change password 36
 - favorites 34
 - FIDO2 keys 37
 - log out 37
 - my requests 32
 - reviews 34
 - settings 35
 - system requirements 19
 - version 35
 - Windows client 35