



# One Identity Safeguard for Privileged Passwords 6.13.1

## User Guide

**Copyright 2022 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](http://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

<b>Introduction</b> .....	<b>5</b>
Introduction to One Identity Safeguard for Privileged Passwords .....	5
Overview of the entities .....	7
<b>System requirements and versions</b> .....	<b>14</b>
Desktop client system requirements .....	15
Web client system requirements .....	16
Web management console system requirements .....	16
Supported platforms .....	17
Licenses .....	29
Long Term Support (LTS) and Feature Releases .....	31
<b>Using the web client</b> .....	<b>33</b>
Home .....	35
My Requests (web client) .....	36
Personal password vault (web client) .....	38
Approvals (web client) .....	42
Reviews (web client) .....	43
Favorites (web client) .....	44
My Settings (web client) .....	45
Change password (web client) .....	47
FIDO2 keys (web client) .....	47
Log out (web client) .....	48
<b>Getting started with the desktop client</b> .....	<b>49</b>
Installing the desktop client .....	49
Starting the desktop client .....	51
Uninstalling the desktop client .....	52
<b>Using the desktop client</b> .....	<b>53</b>
Settings (desktop client) .....	54
User information and log out (desktop client) .....	55
Desktop client favorite request .....	57
Desktop client navigation pane .....	59

Home .....	59
<b>Search box .....</b>	<b>61</b>
Search by attribute .....	62
<b>Privileged access requests .....</b>	<b>64</b>
Configuring alerts .....	65
Toast notifications .....	65
Email notifications .....	66
Password release request workflow .....	66
Requesting a password release .....	66
Taking action on a password release request .....	71
Approving a password release request .....	73
Reviewing a completed password release request .....	75
SSH key release request workflow .....	76
Requesting an SSH key release .....	77
Taking action on an SSH key release request .....	80
Approving an SSH key release request .....	84
Reviewing a completed SSH key release request .....	86
Session request workflow .....	87
About sessions and recordings .....	88
Requesting session access .....	88
Taking action on a session request .....	93
Approving a session request .....	97
Launching the SSH client .....	99
Launching an RDP session .....	101
Reviewing a session request .....	102
Replaying a session .....	104
<b>About us .....</b>	<b>106</b>
Contacting us .....	106
Technical support resources .....	106

## Introduction

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

# Introduction to One Identity Safeguard for Privileged Passwords

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

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

### Safeguard privileged management software suite

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

The Safeguard products' unique strengths are:

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

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

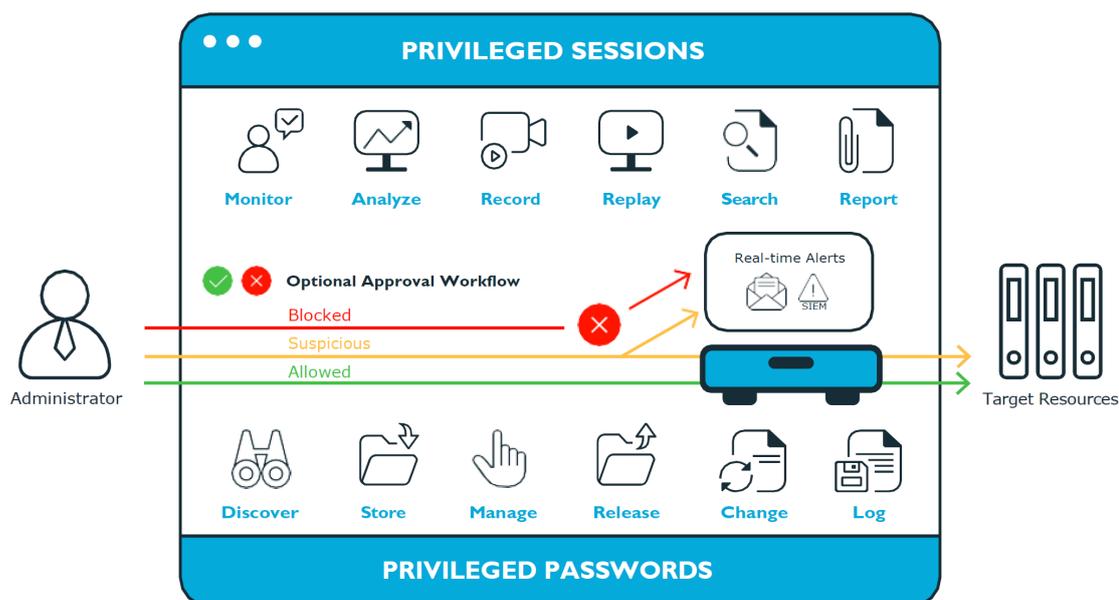
The suite includes the following modules:

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

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

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

**Figure 1: Privileged Sessions and Privileged Passwords**



## Overview of the entities

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

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

### Assets, partitions, and profiles

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

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

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

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

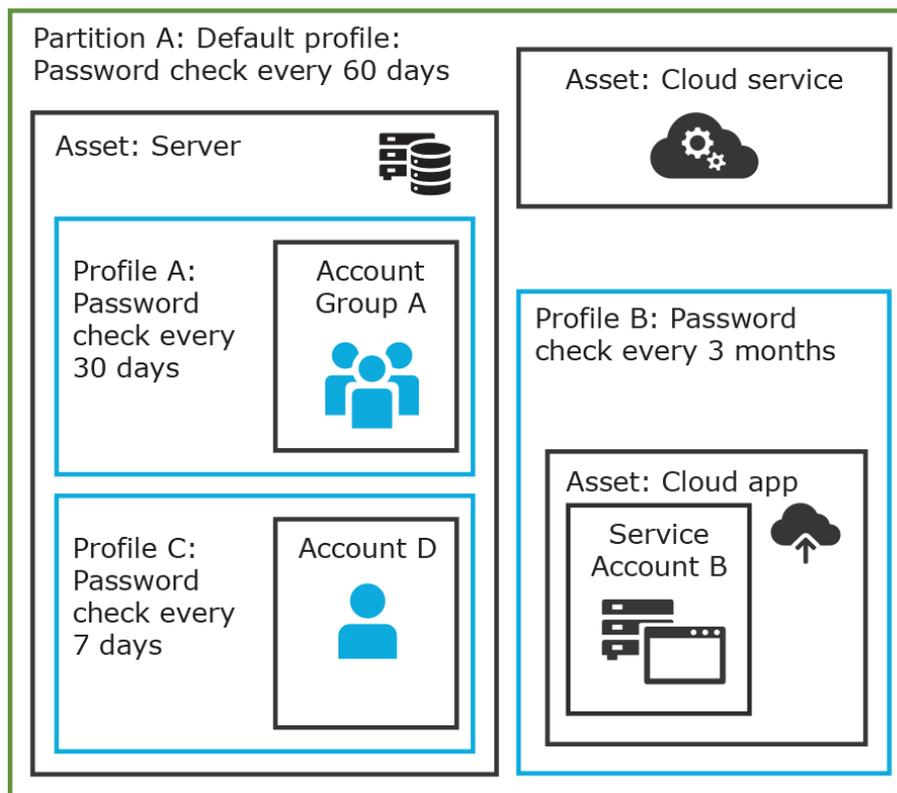
A partition can have multiple profiles, each assigned to different assets, if desired. An account is governed by only one profile. If an account is not explicitly assigned to a profile, the account is governed by the one assigned to the parent asset. If that asset does not have an assigned profile, the partition's default profile is assigned. When updating or restarting a service on a password change, the profile assigned to the asset is used for dependent account service modifications. 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 profile to check and change passwords every 60 days. If you want the password managed for one of those accounts every seven days, you can create another profile and add the individual account to the new profile. Now, Safeguard for Privileged Passwords will check and change all the passwords on this asset every 60 days except for this account, which will change every seven days.

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

**Figure 2: Password control**



**Details: Assets and asset groups**

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

**Details: Partitions and profiles**

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

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

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

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

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

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

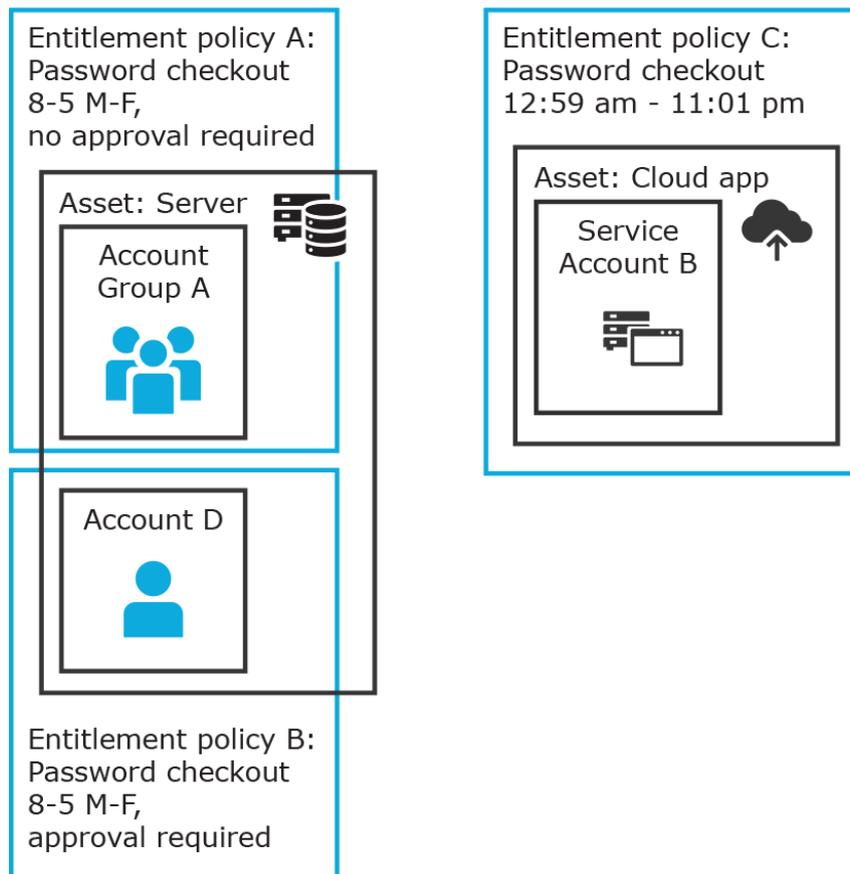
- To define an access request policy for a password or SSH key request, the valid properties in scope are accounts and account groups.
- To define an access request policy for a sessions request, the valid properties in scope are accounts, account groups, assets, and asset groups. If only assets or asset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

Entitlement access request policies may include:

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

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

**Figure 3: Entitlements and accounts**



**Details: Accounts and account groups**

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

**Details: Entitlements and access request policies**

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

## Users and user groups

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

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

Users can be configured for two-factor authentication.

### Details: Users and user groups

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

## Discovery

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

## Access request workflow

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

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

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

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

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

## System requirements and versions

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

- The 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 especially useful for requesters, 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.

**⚠ CAUTION: The Safeguard for Privileged Passwords client version must match the installed Safeguard for Privileged Passwords version.**

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

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

### Bandwidth

It is recommended that connection, including overhead, is faster than 10 megabits per second inter-site bandwidth with a one-way latency of less than 500 milliseconds. If you are using traffic shaping, you must allow sufficient bandwidth and priority to port 655 UDP/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 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 One Identity 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 1: Desktop client requirements**

Component	Requirements
Technology	Microsoft .NET Framework 4.7.2 (or later)
Windows platforms	64-bit editions of: <ul style="list-style-type: none"><li>• Windows 7</li><li>• Windows 8.1</li><li>• Windows 10</li><li>• Windows Server 2008 R2</li><li>• Windows Server 2012</li><li>• Windows Server 2012 R2</li><li>• Windows Server 2016</li><li>• Windows Server 2019</li></ul>

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.

**IMPORTANT:** The Windows 7 Desktop client has additional

Component	Requirements
	<p>requirements in order to enable TLS 1.2. For information, see <a href="#">Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows</a>.</p> <p>Considerations:</p> <ul style="list-style-type: none"> <li>To use FIDO2 two-factor authentication, you will need a web browser that supports the WebAuthn standard.</li> </ul>
Desktop Player	See <i>One Identity Safeguard for Privileged Sessions Safeguard Desktop Player User Guide</i> available at: <a href="#">One Identity Safeguard for Privileged Sessions - Technical Documentation</a> .

## Web client system requirements

**Table 2: Web requirements**

Component	Requirements
Web browsers	<p>Desktop browsers:</p> <ul style="list-style-type: none"> <li>Apple Safari 13.1 for desktop (or later)</li> <li>Google Chrome 80 (or later)</li> <li>Microsoft Edge 80 (or later)</li> <li>Mozilla Firefox 69 (or later)</li> </ul> <p>Mobile device browsers:</p> <ul style="list-style-type: none"> <li>Apple iOS 13 (or later)</li> <li>Google Chrome on Android version 80 (or later)</li> </ul>

## Web management console system requirements

**Table 3: Web kiosk requirements**

Component	Requirements
Web management console	<p>Desktop browsers:</p> <ul style="list-style-type: none"> <li>Apple Safari 13.1 for desktop (or later)</li> <li>Google Chrome 80 (or later)</li> </ul>

Component	Requirements
	<ul style="list-style-type: none"> <li>• Microsoft Edge 80 (or later)</li> <li>• Mozilla Firefox 69 (or later)</li> </ul>

Platforms and versions follow.

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

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

### Safeguard for Privileged Passwords tested platforms

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

**NOTE:** Prior to Safeguard for Privileged Passwords 6.8, the version and architecture information was readonly. It was stored with the platform and formed part of the platform name. As of Safeguard for Privileged Passwords 6.8, this information is no longer associated with the platform. It is now optional, and can be configured on each asset.

A new set of platforms are defined in Safeguard for Privileged Passwords 6.8 to replace the legacy platforms. See the table below for details on how the legacy platforms are mapped to the new platforms.

For customers upgrading from a pre-6.8 version of Safeguard for Privileged Passwords, the legacy platform will automatically be mapped to the corresponding new platform for each existing asset. Following an upgrade, the platform id of each existing asset will have

changed. Some platform names may also have changed. From the desktop UI, only the new platforms are available when creating an asset. By default, the API will also only report the new platforms. For example, a GET request to the following URI will report only the new platforms:

```
https://<appliance>/serve/core/V3/Platforms
```

The legacy platforms still exist within Safeguard for Privileged Passwords for reference, but can only be retrieved using a filter query with the API. For example, the following will retrieve the legacy Active Directory platform:

```
https://<appliance>/serve/core/V3/Platforms?filter=Id%20eq%203
```

## SPP linked to SPS: Sessions platforms

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

Make sure that you do not mix Long Term Supported (LTS) and feature releases. For example, do not link an SPS version 6.0 to an SPP version 6.1.

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

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

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

**Table 4: Supported platforms: Assets that can be managed**

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
ACF2 - Mainframe	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	True
ACF2 - Mainframe LDAP	ACF2 - Mainframe LDAP r14 zSeries ACF2 - Mainframe LDAP r15 zSeries	True	False
Active Directory	Active Directory	True	False
AIX	AIX 6.1 PPC AIX 7.1 PPC AIX 7.2 PPC	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	AIX Other		
Amazon Linux	Amazon Linux 2 x86_64 Amazon Linux Other x86_64	True	True
Amazon Web Services	Amazon Web Services 1	True	False
CentOS Linux	CentOS Linux 6 x86 CentOS Linux 6 x86_64 CentOS Linux 7 x86_64 CentOS Linux 8 x86_64 CentOS Linux Other	True	True
Check Point GAIa (SSH)	Check Point GAIa (SSH) R76 Check Point GAIa (SSH) R77 Check Point GAIa (SSH) R80.30	True	True
Cisco ASA	Cisco ASA 7.X Cisco ASA 8.X Cisco ASA 9.X Cisco ASA Other	True	True
Cisco IOS (510)	Cisco IOS 12.X Cisco IOS 15.X Cisco IOS 16.X Cisco IOS Other	True	True
Cisco ISE	Cisco ISE 2.7 Cisco ISE 3	True	False
Cisco ISE CLI	Cisco ISE CLI 2.7 Cisco ISE CLI 3	True	True
Cisco NX-OS	Cisco NX-OS 9.3(7) Cisco NX-OS 9.3(7a)	True	True
Debian GNU/Linux (511)	Debian GNU/Linux 10 MIPS Debian GNU/Linux 10 PPC Debian GNU/Linux 10 x86 Debian GNU/Linux 10 x86_64	True	True

<b>Platform Name</b>	<b>Legacy Platform (ID)</b>	<b>Supports SPP</b>	<b>Supports SPS Access</b>
	Debian GNU/Linux 10 zSeries		
	Debian GNU/Linux 6 MIPS		
	Debian GNU/Linux 6 PPC		
	Debian GNU/Linux 6 x86		
	Debian GNU/Linux 6 x86_64		
	Debian GNU/Linux 6 zSeries		
	Debian GNU/Linux 7 MIPS		
	Debian GNU/Linux 7 PPC		
	Debian GNU/Linux 7 x86		
	Debian GNU/Linux 7 x86_64		
	Debian GNU/Linux 7 zSeries		
	Debian GNU/Linux 8 MIPS		
	Debian GNU/Linux 8 PPC		
	Debian GNU/Linux 8 x86		
	Debian GNU/Linux 8 x86_64		
	Debian GNU/Linux 8 zSeries		
	Debian GNU/Linux 9 MIPS		
	Debian GNU/Linux 9 PPC		
	Debian GNU/Linux 9 x86		
	Debian GNU/Linux 9 x86_64		
	Debian GNU/Linux 9 zSeries		
	Debian GNU/Linux Other		
Dell iDRAC	Dell iDRAC 7 Dell iDRAC 8 Dell iDRAC 9	True	True
eDirectory LDAP	eDirectory LDAP 9.0	True	False
ESXi	ESXi 5.5 ESXi 6.0 ESXi 6.5 ESXi 6.7 ESXi 7.0	True	False

<b>Platform Name</b>	<b>Legacy Platform (ID)</b>	<b>Supports SPP</b>	<b>Supports SPS Access</b>
F5 Big-IP	F5 Big-IP 12.1.2 F5 Big-IP 13.0 F5 Big-IP 14.0 F5 Big-IP 15.0	True	True
Facebook (Deprecated)	Facebook (Deprecated)		
Fedora	Fedora 21 x86 Fedora 21 x86_64 Fedora 22 x86 Fedora 22 x86_64 Fedora 23 x86 Fedora 23 x86_64 Fedora 24 x86 Fedora 24 x86_64 Fedora 25 x86 Fedora 25 x86_64 Fedora 26 x86 Fedora 26 x86_64 Fedora 27 x86 Fedora 27 x86_64 Fedora 28 x86 Fedora 28 x86_64 Fedora 29 x86 Fedora 29 x86_64 Fedora 30 x86 Fedora 30 x86_64 Fedora 31 x86 Fedora 31 x86_64 Fedora 32 x86 Fedora 32 x86_64 Fedora Other	True	True
Fortinet FortiOS	Fortinet FortiOS 5.2	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	Fortinet FortiOS 5.6 Fortinet FortiOS 6.0 Fortinet FortiOS 6.2		
FreeBSD	FreeBSD 10.4 x86 FreeBSD 10.4 x86_64 FreeBSD 11.1 x86 FreeBSD 11.1 x86_64 FreeBSD 11.2 x86 FreeBSD 11.2 x86_64 FreeBSD 12.0 x86 FreeBSD 12.0 x86_64	True	True
HP iLO	HP iLO 2 x86 HP iLO 3 x86 HP iLO 4 x86 HP iLO 5 x86	True	True
HP iLO MP	HP iLO MP 2 IA-64 HP iLO MP 3 IA-64	True	True
HP-UX	HP-UX 11iv2 (B.11.23) IA-64 HP-UX 11iv2 (B.11.23) PA-RISC HP-UX 11iv3 (B.11.31) IA-64 HP-UX 11iv3 (B.11.31) PA-RISC HP-UX Other	True	True
IBM i (formerly AS400)	IBM i 7.1 PPC IBM i 7.2 PPC IBM i 7.3 PPC IBM i 7.4 PPC	True	True
Junos - Juniper Networks	Junos - Juniper Networks 12 Junos - Juniper Networks 13 Junos - Juniper Networks 14 Junos - Juniper Networks 15 Junos - Juniper Networks 16	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
	Junos - Juniper Networks 17 Junos - Juniper Networks 18 Junos - Juniper Networks 19		
LDAP	OpenLDAP 2.4	True	False
Linux	Other Linux	True	True
macOS	macOS 10.10 x86_64 macOS 10.11 x86_64 macOS 10.12 x86_64 macOS 10.13 x86_64 macOS 10.14 x86_64 macOS 10.15 x86_64 macOS 10.9 x86_64 macOS Other	True	True
MongoDB	MongoDB 3.4 MongoDB 3.6 MongoDB 4.0 MongoDB 4.2	True	False
MySQL	MySQL 5.6 MySQL 5.7 MySQL 8.0	True	False
Oracle	Oracle 11g Release 2 Oracle 12c Release 1 Oracle 12c Release 2 Oracle 18c Oracle 19c	True	False
Oracle Linux (OL)	Oracle Linux (OL) 6 x86 Oracle Linux (OL) 6 x86_64 Oracle Linux (OL) 7 x86_64 Oracle Linux (OL) 8 x86_64 Oracle Linux (OL) Other	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
Other	Other	False	False
Other Directory	Other Directory	True	False
Other Managed	Other Managed	True	False
PAN-OS	PAN-OS 6.0 PAN-OS 7.0 PAN-OS 8.0 PAN-OS 8.1 PAN-OS 9.0	True	True
PostgreSQL	PostgreSQL 10 PostgreSQL 10.2 PostgreSQL 10.3 PostgreSQL 10.4 PostgreSQL 10.5 PostgreSQL 11 PostgreSQL 12 PostgreSQL 9.6	True	False
RACF - Mainframe	RACF - Mainframe z/OS V2.1 Security Server zSeries RACF - Mainframe z/OS V2.2 Security Server zSeries RACF - Mainframe z/OS V2.3 Security Server zSeries	True	True
RACF - RACF - Mainframe LDAP	RACF - Mainframe LDAP z/OS V2.1 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.2 Security Server zSeries RACF - RACF - Mainframe LDAP z/OS V2.3 Security Server zSeries	True	False
Red Hat Enterprise Linux (RHEL)	Red Hat Enterprise Linux (RHEL) 6 PPC Red Hat Enterprise Linux (RHEL) 6 x86 Red Hat Enterprise Linux (RHEL) 6 x86_64	True	True

<b>Platform Name</b>	<b>Legacy Platform (ID)</b>	<b>Supports SPP</b>	<b>Supports SPS Access</b>
	Red Hat Enterprise Linux (RHEL) 6 zSeries		
	Red Hat Enterprise Linux (RHEL) 7 PPC		
	Red Hat Enterprise Linux (RHEL) 7 x86_64		
	Red Hat Enterprise Linux (RHEL) 7 zSeries		
	Red Hat Enterprise Linux (RHEL) 8 PPC		
	Red Hat Enterprise Linux (RHEL) 8 x86_64		
	Red Hat Enterprise Linux (RHEL) 8 zSeries		
	Red Hat Enterprise Linux (RHEL) Other		
Red Hat Directory Server	Red Hat Directory Server 11	True	False
SAP HANA	SAP HANA 2.0 Other	True	False
SAP Netweaver Application Server	SAP Netweaver Application Server 7.3 SAP Netweaver Application Server 7.4 SAP Netweaver Application Server 7.5	True	False
Solaris	Solaris 10 SPARC Solaris 10 x86 Solaris 10 x86_64 Solaris 11 SPARC Solaris 11 x86_64 Solaris Other	True	True
SonicOS	SonicOS 5.9 SonicOS 6.2 SonicOS 6.4 SonicOS 6.5	True	False
SonicWALL SMA or CMS	SonicWALL SMA or CMS 11.3.0	True	False

<b>Platform Name</b>	<b>Legacy Platform (ID)</b>	<b>Supports SPP</b>	<b>Supports SPS Access</b>
SQL Server	SQL Server 2012	True	False
	SQL Server 2014		
	SQL Server 2016		
	SQL Server 2017		
	SQL Server 2019		
SUSE Linux Enterprise Server (SLES)	SUSE Linux Enterprise Server (SLES) 11 IA-64	True	True
	SUSE Linux Enterprise Server (SLES) 11 PPC		
	SUSE Linux Enterprise Server (SLES) 11 x86		
	SUSE Linux Enterprise Server (SLES) 11 x86_64		
	SUSE Linux Enterprise Server (SLES) 11 zSeries		
	SUSE Linux Enterprise Server (SLES) 12 PPC		
	SUSE Linux Enterprise Server (SLES) 12 x86_64		
	SUSE Linux Enterprise Server (SLES) 12 zSeries		
	SUSE Linux Enterprise Server (SLES) 15 PPC		
	SUSE Linux Enterprise Server (SLES) 15 x86_64		
	SUSE Linux Enterprise Server (SLES) 15 zSeries		
SUSE Linux Enterprise Server (SLES) Other			
Sybase (Adaptive Server Enterprise)	Sybase (Adaptive Server Enterprise) 15.7	True	False
	Sybase (Adaptive Server Enterprise) 16		
	Sybase (Adaptive Server Enterprise) 17		
Top Secret -	Top Secret - Mainframe r14 zSeries	True	False

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
Mainframe	Top Secret - Mainframe r15 zSeries Top Secret - Mainframe r16 zSeries		
Top Secret - Mainframe LDAP	Top Secret - Mainframe LDAP r14 zSeries Top Secret - Mainframe LDAP r15 zSeries Top Secret - Mainframe LDAP r16 zSeries	True	True
Twitter (Deprecated)	Twitter (Deprecated)		
Ubuntu	Ubuntu 14.04 LTS x86 Ubuntu 14.04 LTS x86_64 Ubuntu 15.04 x86 Ubuntu 15.04 x86_64 Ubuntu 15.10 x86 Ubuntu 15.10 x86_64 Ubuntu 16.04 LTS x86 Ubuntu 16.04 LTS x86_64 Ubuntu 16.10 x86 Ubuntu 16.10 x86_64 Ubuntu 17.04 x86 Ubuntu 17.04 x86_64 Ubuntu 17.10 x86 Ubuntu 17.10 x86_64 Ubuntu 18.04 LTS x86 Ubuntu 18.04 LTS x86_64 Ubuntu 18.10 x86 Ubuntu 18.10 x86_64 Ubuntu 19.04 x86 Ubuntu 19.04 x86_64 Ubuntu 19.10 x86_64 Ubuntu 20.04 x86_64 Ubuntu Other	True	True

Platform Name	Legacy Platform (ID)	Supports SPP	Supports SPS Access
Windows Desktop	Windows (SSH) 10	True	True
Windows Desktop (SSH)	Windows (SSH) 7		
	Windows (SSH) 8		
Windows Desktop (WinRM)	Windows (SSH) 8.1		
Windows Server	Windows (SSH) Other		
Windows Server (SSH)	Windows (SSH) Server 2008 R2		
	Windows (SSH) Server 2012		
Windows Server (WinRM)	Windows (SSH) Server 2012 R2		
	Windows (SSH) Server 2016		
	Windows (SSH) Server 2019		
	Windows 10		
	Windows 7		
	Windows 8		
	Windows 8.1		
	Windows Other		
	Windows Server 2008		
	Windows Server 2008 R2		
	Windows Server 2012		
	Windows Server 2012 R2		
	Windows Server 2016		
	Windows Server 2019		
	Windows Vista		

**Table 5: Supported platforms: Directories that can be searched**

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

For all supported platforms, it is 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*.

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

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

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

## Licenses

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

### Hardware appliance

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

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

## Virtual appliance Microsoft Windows licensing

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

### Licensing setup and update

#### ***To enter licensing information when you first log in***

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

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

#### ***To configure reminders for license expiration***

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

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

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

#### ***To update the licensing file***

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

#### ***web client: To perform licensing activities***

Go to the licensing page:

1. Navigate to  **Appliance | Licensing**.
  - To upload a new license file, click **+Upload new license file** and browse to select the current license file.
  - To remove the license file, select the license and click  **Remove selected license**.

## **desktop client: To perform licensing activities**

1. Navigate to **Administrative Tools | Settings | Appliance | Licensing**.
  - To upload a new license file, click **+Add License** and browse to select the license file.
  - To update a license file, select the license then select **Update License** in the lower left corner of a module's licensing information pane, select the license file, and click **Open**.

# Long Term Support (LTS) and Feature Releases

Releases use the following version designations:

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

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

**Table 6: Comparison of Long Term Support (LTS) Release and Feature Release**

	<b>Long Term Support (LTS) Release</b>	<b>Feature Release</b>
<b>Release frequency</b>	<b>Frequency:</b> Typically, every 2 years <b>Scope:</b> Includes new features, resolved issues and security updates <b>Versioning:</b> The first digit identifies the LTS and the second digit is a 0 (for example, 6.0 LTS, 7.0 LTS, and so on).	<b>Frequency:</b> Typically, every 3 months <b>Scope:</b> Includes the latest features, resolved issues, and other updates, such as security patches for the OS <b>Versioning:</b> 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).
<b>Maintenance Release</b>	<b>Frequency:</b> Typically, every 3 months during full support <b>Scope:</b> Includes critical resolved issues	<b>Frequency:</b> Only for highly critical issues <b>Scope:</b> Includes highly critical resolved issues

	<b>Versioning:</b> A third digit designates the maintenance LTS Release (for example, 6.0.6 LTS).	<b>Versioning:</b> A third digit designates the maintenance Feature Release (for example, 6.6.1).
<b>Support</b>	Support extends typically 3 years after the original publication date or until the next LTS is published (whichever date is later).	Support extends 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 only work with the same LTS major version of Safeguard for Privileged Sessions (SPS). For the best experience, it is recommended you use the latest supported version.

## Using the web client

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

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



(web client)



(desktop client)

### ***To log into the web client application***

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

1. From your browser, enter the Safeguard for Privileged Passwords URL with the IP address, such as `https://11.1.111.11`.
2. If a login notification displays, click **OK** to accept the notifications and restrictions stated.
3. On the user log in screen, enter your credentials and click **Log in**.

### ***Updating your avatar photo***

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

### ***Using the left navigation menu***

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

The pages available to you display on the left. You will see  **Home** and, based on your role, you may also see the following pages (depending on role, these pages may already be listed in the left navigation pane without having to expand the top level heading):

-  **Access Requests**
  -  **My Requests**
  -  **Personal Password Vault**
  -  **Approvals**
  -  **Reviews**
-  **Appliance Management:**
  -  **Appliance**
  -  **Backup and Retention**
  -  **Certificates**
  -  **Cluster**
  -  **Enable or Disable Services**
  -  **External Integration**
  -  **Real-Time Reports**
  -  **Safeguard Access**
  -  **Search**
-  **Asset Management**
  -  **Accounts**
  -  **Assets**
  -  **Partitions**
  -  **Discovery**
  -  **Profiles**
  -  **Tags**
-  **Security Policy Management**
  -  **Account Groups**
  -  **Application to Application**
  -  **Approval Anywhere**

-  **Cloud Assistant**
-  **Asset Groups**
-  **Entitlements**
-  **Linked Accounts**
-  **User Groups**
-  **User Management**
  -  **Users**
  -  **User Groups**

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

## 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**.

Additional widgets may also be available. For example: **Appliance Resources** and **Cluster Status**.

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

- Customize the information that is displayed on the page. Click  **Settings**.
- Read the **Message of the Day** from the Appliance Administrator.

### Requester's Home page view

Click the **New Request** button 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 an SSH key release](#)
- [Requesting session access](#)

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

For more information, see:

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

The **Favorites** pane displays a list of requests you have marked as a favorite, providing a quick way to request access. For more information, see [Desktop client favorite request](#) on page 57.

### 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 an SSH key 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 completed SSH key release request](#)
- [Reviewing a session request](#)

## My Requests (web client)

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

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

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

### **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 Requests** page.
2. Follow the workflow steps. For more information, see [Requesting a password release](#) on page 66.

### **To create a favorite**

You can create favorites for requests you make often. For more information, see [Favorites \(web client\)](#) on page 44.

### **To view and manage requests**

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

- Click  then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.
- Click **Sort By**  then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.
- Click  sort up or  sort down to sort in ascending or descending order.
- Click  **Filters** to filter by the status.
  - **Available:** Approved requests that are ready to view or copy.
  - **Pending Approval:** Requests that are waiting for approval.
  - **Approved:** Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
  - **Revoked:** Approved requests retracted by the approver. The approver can revoke a request after the request has become available.
  - **Expired:** Requests for which the **Checkout Duration** has elapsed.
  - **Denied:** Requests denied by the approver.

- Click  **Search** to see a list of searchable elements. Or enter search characters. For more information, see [Search box](#).
- If a denied or revoked request has been commented on by an approver, you can click the  button associated with the request to view the comment.

### **To launch web sessions**

The **Launch Web Session** option is available for launching browser-based Safeguard Remote Access sessions from the Safeguard for Privileged Passwords web client. In order to use this button to launch Safeguard Remote Access sessions, some additional requirements must be met:

- Safeguard for Privileged Passwords and Safeguard for Privileged Sessions both must be upgraded to at least 6.12.
- Safeguard for Privileged Passwords must be joined to Starling.
- Safeguard Remote Access and Safeguard for Privileged Sessions may have additional configuration requirements. For more information, see the [Safeguard Remote Access](#) and [Safeguard for Privileged Sessions](#) documentation.

## **Personal password vault (web client)**

The personal password vault extends security and credential protection to business users to store and manage passwords. Users must have the **Personal Passwords** permission granted.

User benefits include:

- Users can store up to 100 personal passwords, set optional expiration dates, and share passwords.
- Users know at a glance the last time they changed their password.
- Users have a history of personal password changes. This is handy if the user changes the password in the vault but not on the target account or if the user needs to work from a backup.
- A password can be shared by the user with one other user. For example, when a user is not available they can give a coworker access to a password. Access can be revoked or the user that has the password shared can opt out of the share.

System users (like the bootstrap admin) cannot create personal accounts.

**IMPORTANT:** The Personal Password Vault permission, like any other permission, can be set explicitly on a user or inherited from a Directory Group. If a user with the Personal Password Vault permission stores one or more personal passwords and then later has the permission revoked, either explicitly or by having been removed from all Directory

Groups from which they inherited it, the user will no longer be able to access  **Personal Password Vault** features. But the user's data within the vault will still be maintained. If at any point the user is granted the Personal Password Vault permission

again, they regain access to all of their existing data.

The **Personal Password Vault** page toolbar functions follow.

**Table 7: Personal Password Vault: Toolbar**

Option	Description
 <b>New Entry</b>	Add an entry to the to the personal password vault.
<b>- Remove Entry</b>	Remove one or more selected entries from the personal password vault. Once an entry is removed, you will not have access to the credentials.
 <b>Edit Entry</b>	Modify the selected entry.
 <b>Information</b>	View information about the selected entry including: <ul style="list-style-type: none"><li>• <b>Name:</b> A meaningful name assigned to the application or account to access. <b>Account Name:</b> The user name for log on authentication. Click  <b>Copy Account Name</b> to copy the name to your clipboard. <b>Password:</b> The secret which you can  <b>Show</b> or  <b>Hide</b> as well as copy by clicking  <b>Copy Password</b>.</li><li>• <b>Expires:</b> The date the password is no longer valid.</li><li>• <b>Notes:</b> Information for the user and anyone sharing the password, such as secondary secrets or other instructions.</li><li>• <b>Sharing:</b> The user name of the person your password is <b>Shared With</b> and the date the <b>Sharing Expires</b>. To change the <b>Sharing Expires</b> date, click  <b>Edit</b>, change the date and then click  <b>Save</b>.</li></ul>
 <b>Share Credentials</b>	Select one or more entries then select the user you want to share credentials with and the date to stop sharing. Users must have this feature enabled to be listed.
 <b>Stop Sharing</b>	Select one or more entries then click  <b>Stop Sharing</b> . If a password is shared by another owner with you, you cannot remove the share but you can opt yourself out of the share.
 <b>History</b>	Thirty days of password history display as a default. You can set a date range for displaying password history by

Option	Description
	<p>selecting <b>From</b> and <b>To</b> values using the  calendar.</p> <p>Or, you can click   <b>Date Range</b> to select set time periods for hours, days, months, or <b>All History</b>.</p> <p>In addition to viewing the Date Changed, you can can  <b>Show</b> or  <b>Hide</b> the password or  <b>Copy Password</b>.</p>
 <b>Copy Account Name</b>	Copy the account name of the selected entry.
 <b>Copy Password</b>	Copy the password of the selected entry.
 <b>Open URL</b>	Click to open the URL web address entered when the password was added or edited.
 <b>Columns</b>	Click to select the columns you want to display.
 <b>Search</b>	Click  to see a list of searchable elements. Or enter search characters. For more information, see <a href="#">Search box</a> .

Entry details for various applications and systems display in the grid.

**Table 8: Personal Password Vault: Passwords grid**

Name	A meaningful name given to the application or account to access, for example Company Twitter.
Account Name	The user name used for log on authentication.
Expires	The date the password expires or blank (no value) if the password does not have an expiration date.
Shared	<p>Display all the following values or click the  filter to select a few values to display:</p> <ul style="list-style-type: none"> <li>• <b>Not Shared</b> if the password is not shared with another user.</li> <li>• <b>Shared</b> if you are sharing the password with another user.</li> <li>• <b>Shared with Me</b> if another user is sharing their password with you.</li> </ul>
Shared With	<p>The user name (and domain name, if applicable) with whom the password is shared; blank if the password is not shared.</p> <p>You can hover over the user name to see the email address for verification.</p>
Owner	The owner of the password.
Sharing Expires	The date sharing expires and the password will no longer be available to the <b>Shared With</b> user.

## To add a password

1. On the  **Personal Password Vault** page, click  **New Entry**.
2. Enter the following values.
  - a. **Name:** Enter a meaningful name for the application or account to access, for example Company Twitter.
  - b. **Account Name:** Enter the user name you use to log on for authentication.
  - c. **Password:** You can type in a password or automatically generate a password. Adding a password is optional. For example, you may want to store information about an application or system in the **Notes** and not store the actual password. The **Notes** limit is 2000 characters.
    - If you type in the password, you can click  **Show** or  **Hide** to view the entry or not. You can also click  **Copy Password** to copy the password to your clipboard.
    - To automatically generate a password, click  **Generate a password**. The password is automatically generated. You can change password rules:
      - i. **Length:** Use the slider or enter a value to reset the required length.
      - ii. **Numbers:** Toggle the requirement to use numbers in the password on  or  off. The password is regenerated per the setting.
      - iii. **Symbols:** Toggle the requirement to use symbols in the password on  or  off. The password is regenerated per the setting.
    - iv. Click  **Regenerate** to generate a new password.
    - v. Click **OK** to save the generated password.
    - vi. Back on the New Entry panel, you can click  **Copy Password** to copy the password to your clipboard.
  - d. **Expires:** It is recommended that you set an expiration date to protect your access. You can enter the date or click the  calendar to select a date.
  - e. **URL:** Enter the web address of the application or system, for example, Amazon.com. Click  **Open URL** to test the link. You can also  **Copy** the URL.
  - f. **Notes:** Enter any free form notes that are helpful for you or for the person with whom you may share the password. You can also use **Notes** for information about an application or system, such as certifications or keys. The limit is 2000 characters.
3. Click **Save**.

### To share your password with another user

1. On the  **Personal Password Vault** page in the grid, select one or more entries to share.
2. Click  **Share Credentials**.
3. On the **Share Credentials** dialog, click **Browse**.
4. On the **Share With...** dialog, users with Personal Passwords permissions are available including their **Display Name**, **Domain**, and **Email Address**. Administrators can add permissions.

Select one user. To search for a user, enter a value in the **Search** text box or click the  icon then make a selection to search by **Domain**, **Display Name**, or **Email Address**. Enter the first letters of the value to display the matches and select the user. Click **OK**.

5. Set the sharing end date which must be between one day and one year. In **Stop Sharing**, enter the date, click the  calendar and select the date, or click  **Sharing Expires** to select a week or month interval. The password will not be available to the user on that date.
6. Click **Share**.

One easy way to change the **Sharing Expires** date later is to select the entry and click  **Information**. Next to the **Sharing Expires** field, click  **Edit**, change the **Sharing Expires** date, then click  **Save**.

### To stop share your password with another user

1. On the  **Personal Password Vault** grid, the Shared column displays **Shared** if you are sharing the password.
2. Select one or more check boxes of entries to stop sharing.
3. Click  **Stop Sharing**. The **Stop Sharing** dialog displays as a warning.
4. Click **Stop Sharing**.

## Approvals (web client)

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

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

- Approve one or more request: Select the requests. Then, click  **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click  **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click  and select the columns you want to see. You can select columns including:
  - **Action:** Displays  **Approve only this request** and  **Deny only this request**.
  - **Requester / Status:** Displays the user name and the status of the approval (for example, **Pending 1 approval**).
  - **Asset / Access Type:** Displays the name of the asset and the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
  - **Account:** Displays the managed account name.
  - **Ticket Number:** Displays the ticket number, if required.
  - **Requested For:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

For more information, see [Approving a password release request](#) on page 73.

## Reviews (web client)

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

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click  **Mark all the selected requests as reviewed**.
  - If a comment is needed, this icon will display as  **One or more of the selected requests requires review comments**. Add the comment. Then, click **Mark as Reviewed**.
- Change the columns that display: Click  **Select columns to display** then select the columns you want to see.

- **Action:** Displays  **This request requires review comments** or  **Mark only this request as reviewed.**
- **Requester:** Displays the user name of the requester.
- **Access Type:** Displays the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
- **Account:** Displays the managed account name.
- **Ticket Number:** Displays the ticket number, if required.
- **Request For/Duration:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

## Favorites (web client)

On your  **Home** or  **My Requests** page, you will see **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 grid view or  for list view.

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

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

### Add a favorite

1. Click  **New Favorite**.
2. On the **New Favorite** 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 61.
  - Once you've selected assets, the number of **Assets selected** displays in the lower left.

- 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 **Favorite Details**, enter a name for the favorite.
  5. Select the color that will be used when displaying the favorite on the  **Home** and  **My Requests** pages.
  6. Click **Save Favorite**.

This access request is then added to your **Favorites**. Once a favorite has been created, you can use and make changes to your favorites by selecting it from

**Favorites** on the  **Home** page or the  **My Requests** page.

**NOTE:** Favorites have unique links, so you can bookmark/copy the link and later access it via that link rather than navigating through the web client

## My Settings (web client)

From **My Settings**, you can set a variety of controls for using the web client. These include page displays, update your information, including email notifications, check the version, or download the Safeguard for Privileged Passwords desktop Windows client. The settings you see are based on your role and permissions.

### Go to My Settings

In the upper right corner, next to your user name, click  then **My Settings** to proceed. On the **My Settings** dialog, the tabs available are based on your role and permissions.

### Using the **General tab**

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

### Using the **My Account tab**

- **Contact Information:** Click  **Edit** to change **Email**, **Work Phone**, or **Mobile Phone**. Click  **Save** to save your changes or click  **Cancel** to revert to the previous setting.
- **Location:** Select your time zone in the drop-down box. Changing your time zone may be prohibited based on your organization's security procedures. If available, choose to:

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

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

- **Manage FIDO2 Keys** (Available if you are required to perform FIDO2 two-factor authentication.): If the FIDO2 feature is enabled, at least one FIDO2 key must be registered. When a key is added, the placeholder name is **Unnamed Key**. You can enter a meaningful name or later edit the name. It is recommended that all users have more than one key registered in case a key is lost or damaged. For existing keys, you will see the name and date each existing key was registered and last used.
  - To change a name, enter the new name, then click  **Save**.
  - To remove a key, click  **Remove** by the key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.
  - To add a key, click  **Register New FIDO2 Key**.
    - a. You will be asked to insert or connect to the new key.
    - b. You will be prompted to reenter your primary credentials for verification.
    - c. Tap or activate your new FIDO2 key that is being registered.
    - d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name, then click  **Save**.

For more information, see [Requiring user to log in using secondary authentication](#).

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

## Change password (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 **My Settings**.
3. Open the **My Account** tab.
4. Click **Change Password**. The password requirements are listed.
5. Enter your **Current Password** and the **New Password** as directed. (Click  **Display** or  **Hide** to view or hide the password as it is entered.)
6. Click **Save** to save your new password.

## FIDO2 keys (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 **My Settings**.
3. Open the **My Account** tab.
4. Click **Manage FIDO2 Keys**. For existing keys, you will see the name and date each existing key was registered and last used.
5. Perform an action:
  - To change a name, enter the new name, then click  **Save**.
  - To remove a key, click  **Remove** by the key. One key must remain registered. If a physical security key is lost, always delete the associated key from Safeguard for Privileged Passwords.
  - To add a key, click  **Register New FIDO2 Key**.
    - a. You will be asked to insert or connect to the new key.
    - b. You will be prompted to reenter your primary credentials for verification.
    - c. Tap or activate your new FIDO2 key that is being registered.
    - d. You may then go back to the **Manage FIDO2 Key** page and give your newly registered key a name, then click  **Save**.

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

## Log out (web client)

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

### **To log out**

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

## 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 33.

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 may 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***

**⚠ CAUTION:** The Safeguard for Privileged Passwords client version must match the installed Safeguard for Privileged Passwords version.

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

### **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. If a login notification displays, click **OK** to accept the notifications and restrictions stated.
5. 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.
6. 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.
7. 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\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

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

- **Windows desktop client:** The desktop client consists of an end-user view and an administrator view. The administrative functionality is dynamically enabled based on the user's permissions. The desktop client user interface information follows.
- **Web client:** The web client is especially useful for requesters, reviewers, and approvers. Many administration functions are available as well. For more information, see [Using the web client](#) on page 33.

**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 55.  
Log events are created based on how the user logged out: `UserLoggedOut` or `InactiveUserLoggedOut`.
-  (**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 54.

# Settings (desktop client)

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

Set the following then click **Done** to save settings.

## Notifications

Control notifications within Safeguard for Privileged Passwords:

- **Run in the System Tray** when you close the application.  
When you select the **Run in the System Tray** check box, you cannot modify the toast notifications check box which follows because you always get notifications. If you deselect the **Run in the System Tray** check box, you can enable or disable toast notifications which follows.
- **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

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.

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

- Enable Requests
- Enable Approvals
- Enable Reviews

## 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:** Links to information regarding the third-party components used in Safeguard for Privileged Passwords.

# User information and log out (desktop client)

Click the user avatar then click **My Account** to modify your personal information, time zone (if allowed), manage email notifications, view current notifications, or log out of Safeguard for Privileged Passwords.

**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.

## **desktop client) User information and log out**

### **To update your personal information or time zone**

1. From the toolbar, select your  user avatar (or the Welcome link with your user name) and choose **My Account**. Perform any of the following:
  - To change your image, select  **Change Photo**.
  - To change your email address, **Work Phone**, or **Mobile Phone**, type into the appropriate box.
  - Under **Location**, you can select a new **Time Zone**. Changing your time zone may be prohibited based on your organization's security procedures. If available, choose to:
    - **Display times in local computer time:** This is the default. It is the time zone set on your local computer.
    - **Display times in my configured time zone:** This is the time zone that is set on this page.
2. Click **Done** to close the My Account pane.

### **To manage the notifications you receive**

1. From the toolbar, select your  user avatar (or the Welcome link with your user name) 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. You can define the types of events for which you want to receive 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. By default, all events are selected. Clear the check box for any events for which you do not want to receive an email notification. You can clear or check all check boxes by selecting or deselecting the check box next to **Events**.
4. Click **OK** to save your selections and close the dialog.
5. 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 (or the Welcome link with your user name) 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 Account pane.

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

### **To change your user password**

1. From the toolbar, select your  user avatar (or the Welcome link with your user name) and choose **My Account**.
2. To change your user password, click **Change Password** and complete the information.
3. Click **Done** to close the My Account pane.

## Log Out

Click the  user avatar (or the Welcome link with your user name) then 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. Click  **Home**.
2. In the **Favorites** pane on the right, click **+ New Favorite**.
3. In the **New Favorite** dialog, specify the following.
  - a. On the **Asset Selection** tab, select the assets to be included in the access request.
  - b. On the **Account & Access Type** tab, highlight 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.
4. Click the **Add to Favorites** button.
5. In the **Add to Favorites** dialog, perform 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.
  - d. Click **Add**. The dialog closes and the new favorite are added to the **Favorites** pane on your **Home** page.

### *To request a favorite*

1. At the top of the **Favorites** pane, click the  button to display the **Request Selected** button.
2. Select the check box to the left of the favorite to be requested.
3. On the **New Access Request** page, edit your selections or enter a required reason or comment before submitting it.
4. Click **Submit Request**.

#### ***To create a new favorite request from an existing favorite***

1. At the top of the **Favorites** pane, click the  button to display the **Request Selected** button.
2. Select the check box to the left of the favorite to be used to create a new favorite. This saves you time entering information.
3. On the **New Access Request** page, edit your selections or enter a required reason or comment before submitting it.
4. At the bottom of the **New Access Request** dialog, click the **Add to Favorites** button. 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.
5. 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.
6. 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.
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.
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.

## 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**.

Additional widgets may also be available. For example: **Appliance Resources** and **Cluster Status**.

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

- Customize the information that is displayed on the page. Click  **Settings**.
- Read the **Message of the Day** from the Appliance Administrator.

## Requester's Home page view

Click the **New Request** button 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 an SSH key release](#)
- [Requesting session access](#)

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

For more information, see:

- [Taking action on a password release request](#)
- [Taking action on an SSH key release request](#)

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

The **Favorites** pane displays a list of requests you have marked as a favorite, providing a quick way to request access. For more information, see [Desktop client favorite request](#) on page 57.

## 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 an SSH key 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 completed SSH key release request](#)
- [Reviewing a session request](#)

## 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 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.
- (Web client only) On the web client, when you click on the search icon in the search bar you will see a drop down of available search attributes (columns) for the grid. This can be used in conjunction with the entered search strings.

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

- By default, results are displayed in alphabetical order.
- Wild cards are not allowed.
- Try using quotes and omitting quotes. As you use the product, you will become familiar with the search requirements for the search fields you frequent. Safeguard may perform a general search (for example, omits quotes) or a literal search (for example, includes quotes). Example scenarios follow:
  - On 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 Rule**. 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. In the web client, if conflicting attributes are entered for the same search (for example, both true and false) then the results will expand to show all matches so long as they fit one of those attributes.
  - When you combine a string search and an attribute search, the order they are entered into the search box matters. The attribute searches can be in any order, but the string search must come after the attribute searches.
  - 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.
  - (Web client only) To search using dates and times in the web client, the following format is used: YYYY-MM-DDThh:mm:ss. For example, if you are searching for an entitlement that expires December 1, 2021 then you would use the following search: ExpirationDate:2021-12-01. To include a minimum and maximum value in a search, use .. to separate two values. For example, if you are searching for an entitlement that expires between December 1, 2021 and December 3, 2021 then you would use the following search: ExpirationDate:2021-12-01..2021-12-03.
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 is displayed.

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

## Search by attribute

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

## API attributes can be searched

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

### Entering the search string

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

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

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

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

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

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

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

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

## Privileged access requests

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

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

As a Safeguard for Privileged Passwords user, your **Home** page provides a quick view to the access request tasks that need your immediate attention. In addition, 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 65.

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 57.
-  Web client: For more information, see [Favorites \(web client\)](#) on page 44.
- Approvers see tasks related to approving (or denying) and revoking access requests.
- Reviewers see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

The following three workflows are available:

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

## Configuring alerts

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

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

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

Using the desktop client, there are two ways to configure One Identity Safeguard for Privileged Passwords to send event alerts to Safeguard for Privileged Passwords users:

- [Toast notifications](#)
- [Email notifications](#)

## Toast notifications

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

- For Local users, you must set your email address correctly in **My Account/My Settings**. For more information, see [My Settings \(web client\)](#) or [User information and log out \(desktop client\)](#).
- For Directory users, set your email correctly in the directory where your user resides.
- Contact your Security Policy Administrator to ensure the access request policies are configured to notify people of pending access workflow events.
- Contact your Appliance Administrator to ensure the SMTP server is configured for email notifications.

## Password release request workflow

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

Typically, a password release request follows this workflow.

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

## Requesting a password release

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending password release workflow events, such as when a password release request is pending, denied, or revoked, and so forth. For more information, see [Configuring alerts](#) on page 65.

### To request a password release ( web client)

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

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

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

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

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

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

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

- **Access Type:** The type of access request appears in the **Access Type** column. If the type is a drop-down, multiple access request types are available. Open the drop-down and select the access type, for example, **Password**, **RDP**, **SSH**, **SSH Key**, or **Telnet**.
- **Account Description:** (When applicable) The description of the account.
- **Asset Description:** (When applicable) The description of the asset.

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

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

- a. **Emergency Access:** If the policy has emergency access enabled, select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval.
  - b. **When:** Select one of the following options:
    - i. **Now:** If selected, the request is immediately created.
    - ii. **Later:** If selected, fields will appear allowing you to enter a specific date and time for the request in the user's local time.
  - c. **How Long:** Based on the policy, do one of the following:
    - View the **Checkout Duration**.
    - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy.
  - d. **Ticket Number:** If the policy requires a ticket number, enter a ticket number. If multiple accounts are in the request and one or more require a ticket number, the ticket number is applied to all of the requests associated with this access request. This feature is set up through the desktop client.
  - e. **Reason:** If the policy requires a reason, enter a reason. If multiple accounts are in the request and one or more require a reason. The reason is applied to all of the requests associated with this access request.  
  
Select the **Description** down arrow to view the description defined for the selected reason.
  - f. **Comment:** If required, enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 1000 characters.
5. To save the access request as a favorite, select the **Save this request as a favorite** check box and enter a name for the request.

This access request is then added to your **Favorites**. In the web client, favorites are displayed on the  **Home** page and the  **My Requests** page. For more information, see [Favorites \(web client\)](#) on page 44.

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

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

When the request has been approved, you can use the password. For more information, see [Taking action on a password release request](#) on page 71.

## To request a password release ( desktop client)

1. 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.

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

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

You must have the  column, **Availability** check box selected to show accounts that are available.

- **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, for example, **Password**, **RDP**, **SSH**, **SSH Key**, or **Telnet**.

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**. 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 57.
6. After entering the required information, click **Submit Request**.
- The **Results** dialog displays the access requests submitted and whether a request was successful. If unsuccessful due to usage restrictions, a message returns the time available.

When the request has been approved, you can use the password. For more information, see [Taking action on a password release request](#) on page 71.

# 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.

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

### **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 resize 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.

## **web client) To take action on a password release request**

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

- If a denied or revoked request has been commented on by an approver, you can click the  button associated with the request to view the comment.
2. You can take any of the following actions on the password release request:
- **Available request:** Make selections on the request based on your user interface.
    - The name, account, and remaining time is displayed.
    - If your browser allows, click  **Copy** to check out the password. This puts the password onto your clipboard, ready for you to use. Or, click  **Show** to check out the password and view the password. A password displays on your screen for 20 seconds. The web client displays up to 10,000 characters before truncating the password, however the API allows any set password payload below 1MBb. If the password changes while you have it checked out, and your current request is still valid, select either  **Copy** or  **Show** again to obtain the new password.
    - Select  **Hide** to conceal the information from view.
    - Once you are done working, click  **Check-In Request** to complete the password check out process.
  - **Approved request:** Select  **Cancel Request** to remove the request. A password release request changes from **Approved** to **Available** when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
  - **Pending request:** Select  **Cancel Request** to remove the request.
  - **Revoked request:** Select **Resubmit** to request the password again.
  - **Expired request:** Select  **Remove Request** to delete the request from the list.
  - **Denied request:** Select **Resubmit** to request the password again. Select  **Remove Request** to delete the request from the list.

## Approving a password release request

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

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

Any eligible approver can deny a password release request after it has already been approved or auto-approved. Once disallowed, the requester will no longer have access to

the password, but they are given another opportunity to request that password again. The requester receives an email notifying them that the request was denied.

Safeguard for Privileged Passwords can be configured to notify you of a password release request that requires your approval. For more information, see [Configuring alerts](#) on page 65.

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

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

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click  **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click  **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click  and select the columns you want to see. You can select columns including:
  - **Action:** Displays  **Approve only this request** and  **Deny only this request**.
  - **Requester / Status:** Displays the user name and the status of the approval (for example, **Pending 1 approval**).
  - **Asset / Access Type:** Displays the name of the asset and the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
  - **Account:** Displays the managed account name.
  - **Ticket Number:** Displays the ticket number, if required.
  - **Requested For:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

### (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 resize 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 65.

### (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 by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click  **Mark all the selected requests as reviewed.**
  - If a comment is needed, this icon will display as  **One or more of the selected requests requires review comments.** Add the comment. Then, click **Mark as Reviewed.**
- Change the columns that display: Click  **Select columns to display** then select the columns you want to see.

- **Action:** Displays  **This request requires review comments** or  **Mark only this request as reviewed.**
- **Requester:** Displays the user name of the requester.
- **Access Type:** Displays the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
- **Account:** Displays the managed account name.
- **Ticket Number:** Displays the ticket number, if required.
- **Request For/Duration:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

### (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 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 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.

## SSH key release request workflow

One Identity Safeguard for Privileged Passwords provides secure control of managed accounts by storing SSH keys until they are needed, and releases them only to authorized

persons. Then, Safeguard for Privileged Passwords automatically updates the account SSH keys based on configurable parameters.

Typically, an SSH key release request follows this workflow.

1. **Request:** Users that are designated as an authorized user of an entitlement can request SSH keys for any account in the scope of that entitlement's policies.
2. **Approve:** Depending on policy configuration, approval can be automatic or require the consent of one or more users which provides closer control over system accounts.
3. **Review:** The Security Policy Administrator can optionally configure an access request policy to require a review of completed SSH key release requests for accounts in the scope of the policy.

## Requesting an SSH key release

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending SSH key release workflow events, such as when an SSH key release request is pending, denied, or revoked, and so forth. For more information, see [Configuring alerts](#) on page 65.

### To request an SSH key release (🌐 web client)

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

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

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

3. **NOTE:** Use the **Columns** button to select the columns to display.

- **Asset:** The display name of the managed system.
- **Account:** The available account appears in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.
- **Access Type:** The type of access request appears in the **Access Type** column. If the type is a drop-down, you can click the drop-down then multiple access request types are available. Click the drop-down and select the access

type, in this case, **SSH Key**.

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

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

4. Click **Next**.

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

- Emergency Access:** If the policy has emergency access enabled, select this option to gain immediate emergency access to this SSH key. When you use **Emergency Access**, the request requires no approval.
- When:** Select one of the following options:
  - Now:** If selected, the request is immediately created.
  - Later:** If selected, fields will appear allowing you to enter a specific date and time for the request in the user's local time.
- How Long:** Based on the policy, do one of the following:
  - View the **Checkout Duration**.
  - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy.
- 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.
- 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.
- Comment:** If required, enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 1000 characters.

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

This access request is then added to your **Favorites**. In the web client, favorites are displayed on the  **Home** page and the  **My Requests** page. For more information, see [Favorites \(web client\)](#) on page 44.

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

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

When the request has been approved, you can use the SSH key. For more information, see [Taking action on an SSH key release request](#) on page 80.

### To request an SSH key release ( desktop client)

2. 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.

3. 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 per request.
4. 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, you can click the link then multiple access request types are available. Select the hyperlink and select the access type, in this case, **SSH Key**.

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

5. 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 SSH key. 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 SSH key. 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 SSH key. 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.

6. 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**. 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 57.

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

The **Results** dialog displays the access requests submitted and whether a request was successful. If unsuccessful due to usage restrictions, a message returns the time available.

When the request has been approved, you can use the SSH key. For more information, see [Taking action on an SSH key release request](#) on page 80.

## Taking action on an SSH key release request

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

## To take action on an SSH key release request ( web client)

1. From the web client, click  **My Requests**. Use any of the following methods to control the request displayed:
  - Click  then select **Check-In All Available** to check-in all the available requests, **Clear All** to remove all requests, or **Cancel All Pending Time Requested** to cancel and remove all pending requests.
  - Click **Sort By**  then select to sort by **Account Name**, **Asset Name**, **Due Next**, **Expiring Next**, **Most Recent**, or **Status**.
  - Click  sort up or  sort down to sort in ascending or descending order.
  - Click  **Filters** to filter by the status.
    - **Available**: Approved requests that are ready to view or copy.
    - **Pending Approval**: Requests that are waiting for approval.
    - **Approved**: Requests that have been approved, but the check out time has not arrived. Or, for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
    - **Revoked**: Approved requests retracted by the approver. The approver can revoke a request after the request has become available.
    - **Expired**: Requests for which the **Checkout Duration** has elapsed.
    - **Denied**: Requests denied by the approver.
  - Click  **Search** to see a list of searchable elements. Or enter search characters. For more information, see [Search box](#).
  - If a denied or revoked request has been commented on by an approver, you can click the  button associated with the request to view the comment.
2. You can take any of the following actions on the SSH key release request:
  - Available request: Make selections on the request based on your user interface.
    - a. The name, account, and remaining time is displayed. Click on the tile to see additional information or use the  **Fetch SSH Details** button.
    - b. The **Format** displays and can be selected, if necessary. Formats include **OpenSSH**, **SSH2**, and **PuTTY**. The **Format** chosen is preselected as the default for the next access request.
    - c. Click  **Checkout SSH Key** to check out the SSH key. This puts the SSH key onto your clipboard, ready for you to use.
    - d. Click  **Start SSH Session** to launch the session.
    - e. **Private Key**: You can click  **Save** or  **Copy**.

- f. **Passphrase:** You can click  **Show** or  **Copy** if **Passphrase Protect SSH Key** was selected on when creating an access request policy. For more information, see Access Config tab in the *Safeguard for Privileged Passwords Administration Guide*.
- g. The following types of information may display based on the format you select.

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

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

- h. Once you are done working, click  **Check-In Request** to complete the SSH key check out process.
- **Approved** request: Select  **Cancel Request** to remove the request.  
An SSH key release request changes from **Approved** to **Available** when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
- **Pending** request: Select  **Cancel Request** to remove the request.
- **Revoked** request: Select **Resubmit** to request the SSH key again.  
Select  **Remove** to delete the request from the list.
- **Expired** request: Select  **Remove Request** to delete the request from the list.
- **Denied** request: Select **Resubmit** to request the SSH key again.  
Select  **Remove Request** to delete the request from the list.

### To take action on an SSH key release request ( **desktop client**)

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 resize 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 SSH key 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 SSH key release request. Take the following actions on SSH key release requests:
- **Available** request: Make selections on the request based on your user interface.
    1. The name, **Account** and **Remaining** time displays.
    2. The **Format** displays and can be selected, if necessary. Formats include **OpenSSH,SSH2**, and **PutTY**. The **Format** chosen is preselected as the default for the next access request.
    3. Click  **Checkout SSH Key** to check out the SSH key. This puts the SSH key into your copy buffer, ready for you to use.
    4. **Private Key:** You can click  **Save** or  **Copy**.
    5. **Passphrase:** You can click  **Show** or  **Copy** if **Passphrase Protect SSH Key** was selected on when creating an access request policy. For more information, see Access Config tab in the *Safeguard for Privileged Passwords Administration Guide*.
    6. To view more detail, select **More Info** . The following types of information may display based on the format you select.
      - **SHA-1 Fingerprint**
      - **MD5 Fingerprint**
      - **Public Key:** You can click  **Save** or  **Copy**.

If the SSH key changes while you have it checked out, and your current request is still valid, you can select the following to obtain an new SSH key, as available:  **Save**,  **Copy**, or  **Show**.
    7. Once you are done working, click  **Check-In** to complete the SSH key check out process. (You may need to close **More Info** .)

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

## Approving an SSH key release request

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

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

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

Safeguard for Privileged Passwords can be configured to notify you of an SSH key release request that requires your approval. For more information, see [Configuring alerts](#) on page 65.

### (web client) To approve or deny an SSH key release request

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

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click  **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.

- Deny one or more request: Select the requests. Then, click  **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click  and select the columns you want to see. You can select columns including:
  - **Action:** Displays  **Approve only this request** and  **Deny only this request**.
  - **Requester / Status:** Displays the user name and the status of the approval (for example, **Pending 1 approval**).
  - **Asset / Access Type:** Displays the name of the asset and the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
  - **Account:** Displays the managed account name.
  - **Ticket Number:** Displays the ticket number, if required.
  - **Requested For:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

### (desktop client) To approve or deny an SSH key 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 resize 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:** SSH key 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 SSH key release request.
4. Take the following actions on SSH key release requests:
  - **Pending:** Select  to **Approve** or  to **Deny** an SSH key release request. Optionally, enter a comment of up to 255 characters.
  - **Pending Additional Approvers:** Select  to **Deny** an SSH key release request. Optionally, enter a comment of up to 255 characters.
  - **Approved:** Select  to **Deny** or **Revoke** an approved request.

# Reviewing a completed SSH key release request

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

You can configure Safeguard for Privileged Passwords to notify you of an SSH key release request that requires your review. For more information, see [Configuring alerts](#) on page 65.

## (web client) To review a completed SSH key release request

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

- View details by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click  **Mark all the selected requests as reviewed.**
  - If a comment is needed, this icon will display as  **One or more of the selected requests requires review comments.** Add the comment. Then, click **Mark as Reviewed.**
- Change the columns that display: Click  **Select columns to display** then select the columns you want to see.
  - **Action:** Displays  **This request requires review comments** or  **Mark only this request as reviewed.**
  - **Requester:** Displays the user name of the requester.
  - **Access Type:** Displays the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
  - **Account:** Displays the managed account name.
  - **Ticket Number:** Displays the ticket number, if required.
  - **Request For/Duration:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

## (desktop client) To review a completed SSH key 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 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 SSH key release request.
3. Take the following action on SSH key 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 SSH key 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 close connections.

Typically a session request follows the workflow below:

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

# About sessions and recordings

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

**NOTE:** PuTTY is used to launch the SSH client for SSH session requests and 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**) or in the web client (**Appliance Management | Enable or Disable Services**).

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

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

## Requesting session access

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending access request workflow events, such as when a session request is pending, denied, or revoked, and so on. For more information, see [Configuring alerts](#) on page 65.

## To request session access ( web client)

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

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

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

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

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

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

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

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

- **Access Type:** The type of access request appears in the **Access Type** column. If the type is a drop-down, multiple access request types are available. Select the hyperlink and select the access type.
- **Account Description:** (When applicable) The description of the account.
- **Asset Description:** (When applicable) The description of the asset.

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

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

- a. **Emergency Access:** If the policy has emergency access enabled, select this option to gain immediate emergency access to this password. When you use **Emergency Access**, the request requires no approval.
  - b. **When:** Select one of the following options:
    - i. **Now:** If selected, the request is immediately created.
    - ii. **Later:** If selected, fields will appear allowing you to enter a specific date and time for the request in the user's local time.
  - c. **How Long:** Based on the policy, do one of the following:
    - View the **Checkout Duration**.
    - If the **Allow Requester to Change Duration** option is enabled in the policy, you can set the days, hours, and minutes that you want to use the password. This overrides the **Checkout Duration** set in the access request policy.
  - d. **Ticket Number:** If the policy requires a ticket number, enter a ticket number. If multiple accounts are in the request and one or more require a ticket number, the ticket number is applied to all of the requests associated with this access request. This feature is set up through the desktop client.
  - e. **Reason:** If the policy requires a reason, enter a reason. If multiple accounts are in the request and one or more require a reason. The reason is applied to all of the requests associated with this access request.  
  
Select the **Description** down arrow to view the description defined for the selected reason.
  - f. **Comment:** If required, enter information about this request. When multiple accounts are specified in the request, if any of the selected accounts require a comment, you must enter a comment. The comment will be applied to all of the requests associated with this access request. The limit is 255 characters.
5. To save the access request as a favorite, select the **Save this request as a favorite** check box and enter a name for the request.

This access request is then added to your **Favorites**. In the web client, favorites are displayed on the  **Home** page and the  **My Requests** page. For more information, see [Favorites \(web client\)](#) on page 44.

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

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

When the request has been approved, you can use the password. For more information, see [Taking action on a password release request](#) on page 71.

## To request session access ( desktop client)

1. 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 or SSH key. 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 or SSH session. 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 duration of the check out; 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 or SSH session 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**. 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 57.

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.

## If the session does not launch

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

- Please try again. The linked sessions module state is currently down or may be in a locked state. This message may mean one of the following:
  - SPP could not contact SPS. Try again so the request can be redirected to another managed host in the SPS cluster.
  - The SPS configuration is locked. Try again because this condition is typically because the SPS administrator is making configuration changes to the SPS appliance at the same time that a new access request is being created or a session is being launched.
- Missing the session connection policy. or  
The selected Access Request Policy cannot be used to initiate a session from SPP. The highest priority policy must be associated with a valid SPS connection policy.  
Check the connection policy configuration. In the web client, go to **Security Policy Management | Entitlements | (edit) | Access Request Policies** to add a valid connection policy; or 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.

## To take action on a session request ( web client)

1. From the web client, click  **My Requests**.
2. Search to find what you need. For more information, see [Search box](#) on page 61.
3. Click  **Filters** to filter by the status.
  - **All**: Requests in all states.
  - **Available**: Approved requests that are ready (that is, a session that can be launched).
  - **Pending Approval**: Requests that are waiting for approval.
  - **Approved**: Requests that have been approved, but the check out time has not arrived.
  - **Revoked**: Approved requests retracted by the approver.
    - The approver can revoke a request after it is available.
    - When a user with Security Policy Administrator permissions revokes a live session, the active session is closed.
  - **Expired**: Requests for which the **Checkout Duration** has elapsed.
  - **Denied**: Requests denied by the approver.
4. Depending on the type of request, additional information may be available by clicking the tile.
5. You can take the following actions on session requests, depending on the state.
  - Available request: If the password or SSH key changes while you have it checked out, and your current request is still valid, select either  **Copy** or  **Show** again to obtain the new password or SSH key, if enabled by your Administrator.
    - For SSH and RDP accounts:
      - The **▶Start RDP Session/Start SSH Session** options are available only if enabled by user preferences. Click to launch the SSH client or RDP connection. For more information, see [Launching the SSH client](#) or [Launching an RDP session](#).
      - Click  **Check-In** to complete the check out process once you have ended your session.
      - In addition, you can use the following buttons to view or copy information into the dialog that contains the credentials needed to launch the session.
        - Click  **Copy** to check out and copy the credential.
        - Click  **Show** to check out the credential and view the credential.
    - For telnet or TN3270/TN5250 over telnet accounts, the fields needed are based on the terminal service application in use:

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

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

- 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 resize 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 closed.
  - **Expired:** Requests for which the check out 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 or SSH key changes while you have it checked out, and your current request is still valid, select either  **Copy** or  **Show** again to obtain the new password or SSH key, if enabled by your Administrator. **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 or SSH key. Then, paste the information in the log in screen.
- If the terminal service application requires more information for log in (for example, TN3270/TN5250 over telnet):
  - Click  **Show** to display values that may include **Vault Address** (the SPP address), a one-time **Token, Username, Asset**, and **Sessions Module** (the SPS address).
  - Click  **Copy** by any of the values to copy a single value. Or, you can click  **Copy** at the right of all values to copy the entire the connection string, if that is required by your terminal service application.
  - Paste the necessary information into your terminal service application.
- Click  **Check-In Request** to complete the password or SSH key check out process. This makes the session request available to reviewers.
- Click  **Hide** to conceal the information from view.
- **Approved:** Select  **Cancel** 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 or SSH key 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 65.

## (web client) To approve or deny a session request

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

- View details by selecting a request then looking at the details display on the right of the page.
- Approve one or more request: Select the requests. Then, click  **Approve all selected requests** to approve all the requests you selected. Optionally, enter a comment.
- Deny one or more request: Select the requests. Then, click  **Deny all selected requests** to deny all the requests you selected. Optionally, enter a comment.
- Change the columns that display: Click  and select the columns you want to see. You can select columns including:
  - **Action:** Displays  **Approve only this request** and  **Deny only this request**.
  - **Requester / Status:** Displays the user name and the status of the approval (for example, **Pending 1 approval**).
  - **Asset / Access Type:** Displays the name of the asset and the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
  - **Account:** Displays the managed account name.
  - **Ticket Number:** Displays the ticket number, if required.
  - **Requested For:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

## (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 resize the window.

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

- 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.

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

State	Actions
Pending	Select  to <b>Approve</b> or <b>Deny</b> a sessions request. Optionally, enter a comment of up to 255 characters.
Pending Additional Approvers	Select  to <b>Deny</b> a sessions request. Optionally, enter a comment of up to 255 characters.
Approved	Select  to <b>Deny</b> or <b>Revoke</b> an approved request. You can revoke a request between the time the requester views it and checks it in. Any eligible approver can deny an access request after it has already been approved or auto-approved. Once disallowed, the requester will no longer be able to access the requested session, but 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 <a href="#">Configuring alerts</a> on page 65.

## 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***

- 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/Start SSH Session** button associated with the asset name.

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

- 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** or **SSH Key** to perform the following tasks.
    - **View:** To view the password or SSH key.
    - **Copy:** To copy the password or SSH key to your copy buffer, which can then be pasted into the Password or SSH Key field of the **PuTTY Configuration** dialog.
    - **Help:** To copy the value into the Password or SSH Key field of the **PuTTY Configuration** dialog.
    - **NOTE:** The **Password** or **SSH Key** 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 closed. However, as long as the request is in an **Available** state, you can launch the session again to resume your tasks.

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

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:
  -  (web client) In the web client:
    - **NOTE:** The ► **Start RDP Session** option is available only if enabled by user preferences.
    - If you have an application registered (`rdp://` for RDP sessions), you can click the ► **Start RDP Session** button associated with the asset name then click **Connect**. See [KB 313918](#) for details on application registration. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.
    - If you do not have an application registered, download the RDP launch file instead of using the ► **Start RDP Session** button. A password must be entered and we recommend `sg`. A blank password will cause the session to fail.
  -  (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.

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

**NOTE:** The **Password** or **SSH Key** field only appears if the **Include password or SSH key release with session requests** option (Access Config tab) is selected in the entitlement's access request policy. For more information, see Access Config tab in the *Safeguard for Privileged Passwords Administration Guide*.

### **Begin your RDP session and close the session**

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

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 65.

### **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 by selecting a request then looking at the details display on the right of the page, including the workflow.
- Mark one or more request as reviewed: Select the requests. Do the following:
  - If no comment is needed, click  **Mark all the selected requests as reviewed.**
  - If a comment is needed, this icon will display as  **One or more of the selected requests requires review comments.** Add the comment. Then, click **Mark as Reviewed.**
- Change the columns that display: Click  **Select columns to display** then select the columns you want to see.
  - **Action:** Displays  **This request requires review comments** or  **Mark only this request as reviewed.**
  - **Requester:** Displays the user name of the requester.
  - **Access Type:** Displays the type of access (for example, **Password, SSH Key, RDP, SSH, or Telnet**).
  - **Account:** Displays the managed account name.
  - **Ticket Number:** Displays the ticket number, if required.
  - **Request For/Duration:** Displays the date and time as well as the window of availability (for example, **March 20, 2021 9:56 AM 2 hours**).
- **Search:** For more information, see [Search box](#) on page 61.

## (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 linking 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.

### (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.
3. Depending on the source of the session, you will see one of the following buttons:
  -  **Link:** For sessions recorded on the earlier embedded SPP sessions module. Click  **Link**. You can play the session if it is archived. If the session has not been archived, you will see a message like: The session recording is

unavailable until it is archived, please refer to the documentation. For more information, see SPP and SPS sessions appliance join guidance in the *Safeguard for Privileged Passwords Administration Guide*.

- **▶ Play**: for sessions recorded from and stored on SPS. Continue to the next step.
4. Click **▶ Play** to launch the Desktop Player to play a session recorded from SPS. 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](#).**

5. 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.
6. 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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product