



One Identity Safeguard for Privileged Passwords 2.5

User Guide

Copyright 2018 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

-  **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.
-  **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO:** An information icon indicates supporting information.

Contents

Introduction	5
Introduction to One Identity Safeguard for Privileged Passwords	5
Key features	6
What's new in version 2.1	8
What's new in version 2.2	10
What's new in version 2.3	13
What's new in version 2.4	13
What's new in version 2.5	14
System requirements	16
Desktop client system requirements	16
Web client system requirements	17
Product licensing	18
Installing the One Identity Safeguard for Privileged Passwords desktop client	19
Installing the desktop client	19
Starting the desktop client	20
Uninstalling the desktop client	20
Getting acquainted with the console	21
Toolbar controls	21
Console Settings	22
User avatar	23
Navigation pane	24
Home	24
Search box	26
Privileged access requests	29
Creating, editing, or removing a favorite request	30
Configuring alerts	32
Toast notifications	32
Email notifications	33
Password release request workflow	33

Requesting a password release	33
Taking action on a password release request	36
Approving a password release request	37
Reviewing a completed password release request	39
Session request workflow	39
About sessions and recordings	40
Requesting session access	41
Taking action on a session request	43
Approving a session request	45
Launching the SSH client	46
Launching an RDP session	47
Reviewing a session request	49
Replaying a session	50
Safeguard Desktop Player	51
Recording navigation	54
Exporting video	56
Key descriptions	57
About us	59
Contacting us	59
Technical support resources	59
Index	60

Introduction

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

Introduction to One Identity Safeguard for Privileged Passwords

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

The privileged management software provided with One Identity Safeguard for Privileged Passwords consists of the following modules:

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

privileged account misuse, facilitate compliance, and accelerate forensics investigations.

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

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

Key features

The following key features are available when you have both Safeguard for Privileged Passwords and the embedded sessions module running on the same hardened secure appliance.

NOTE: If a Safeguard Sessions Appliance is joined to Safeguard for Privileged Passwords, session recording is handled via Safeguard for Privileged Session.

Table 1: One Identity Safeguard for Privileged Passwords key features

Feature	Description
Release control	Manages password requests from authorized users for the accounts they are entitled to access via a secure web browser connection with support for mobile devices.
Workflow engine	A workflow engine supports time restrictions, multiple approvers and reviewers, emergency access, and expiration of policy. It also includes the ability to input reason codes and/or integrate directly with ticketing systems. An access request can be automatically approved or require multiple sets of approvals.
Discovery	Quickly discover any privileged account or system on your network with host, directory and network-discovery options.
Approval Anywhere	Leveraging One Identity Starling, you can approve or deny any access request anywhere without being on the VPN.
Favorites	Quickly access the passwords that you use the most right from the Home screen.
Always online	Safeguard for Privileged Passwords Appliances can be clustered to

Feature	Description
	<p>ensure high availability. Passwords and sessions can be requested from any appliance in a Safeguard for Privileged Passwords cluster.</p> <p>This distributed clustering design also enables the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.</p>
RESTful API	<p>Safeguard for Privileged Passwords uses a modernized API based on a REST architecture which allows other applications and systems to connect and interact with it. The API enables quick and easy integration with diverse systems and applications spanning many programming languages.</p>
Activity Center	<p>Using the Activity Center, you can quickly and easily view all actions executed by Safeguard for Privileged Passwords users and integrated processes. Activity Center reports can be searched, customized and filtered to zero-in on the actions of a single user or to audit a variety of actions across a subset of departments. In addition, you can schedule queries, and save or export the data.</p>
Two-factor authentication support	<p>Protecting access to passwords with another password isn't enough. Enhanced security by requiring two-factor authentication to Safeguard for Privileged Passwords. Safeguard for Privileged Passwords supports any Radius-based 2FA solution and One Identity's Starling Two-Factor Authentication service.</p>
Smartcard support	<p>Authentication of your privileged users can be integrated with Microsoft's Active Directory support for Smartcards or manually uploaded to the Safeguard for Privileged Passwords Appliance itself.</p>
Full session audit, recording and replay	<p>Every packet sent and action that takes place on the screen -- including mouse movements, clicks and keystrokes -- is recorded and available for review. The time and content of the session are cryptographically signed for forensics and compliance purposes. Only actual activity is recorded, and recordings are compressed to a fraction of the size required by other solutions to minimize offline storage requirements.</p>
Proxy access	<p>The embedded sessions module proxies all sessions to target resources. Since users have no direct access to resources, the enterprise is protected against viruses, malware and other dangerous items on the user's system. The embedded sessions module can proxy and record Unix/Linux, Windows, network devices, firewalls, routers and more.</p>
Work the way you want	<p>The embedded sessions module enables administrators to choose their access tools and tool preferences (for example, PuTTY) when</p>

Feature	Description
	gaining access to privileged sessions. This creates a frictionless solution that gives administrators the access they need while meeting compliance and security regulations.
Command detection	<p>During a privileged session, Safeguard for Privileged Passwords can detect commands that are being run on the target host. All actions are logged and can be sent out, if configured, to various logging mechanisms (syslog, email, SNMP).</p> <p>NOTE: For an RDP session, Safeguard for Privileged Passwords can detect the title of any window that is opened on the desktop during a privileged session.</p>
Indexing	Create a searchable list of commands and programs that were run during the recorded session. Auditors have a quick and easy view to session activities.
Auto-login	Sessions access request launch and auto-login enhances security and compliance by never exposing the account credentials to the user.
Protocol support	The embedded sessions module provides full support for the SSH and RDP protocols. In addition, administrators can decide what options within the protocols they want to enable/disable.
Secure access to legacy systems	Use smartcard, two-factor authentication or other strong authentication methods to gain access to systems. Because Safeguard for Privileged Passwords acts as a gateway or proxy to the system, it enables strong authentication to targets that cannot or do not support those methods natively.

What's new in version 2.1

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

Table 2: Safeguard 2.1: Features and enhancements

Feature/Enhancement	Description
Additional platform support	<p>Safeguard for Privileged Passwords now supports the management of assets on the following additional platforms:</p> <ul style="list-style-type: none"> • ACF2 - Mainframe r14 and r15 • ACF2 - Mainframe LDAP r14 and r15 • Debian GNU/Linux 9

Feature/Enhancement	Description
---------------------	-------------

	<ul style="list-style-type: none">• ESXi 6.5• Fedora 26• Fortinet FortiOS 5.2 and 5.6• F5 Big-IP 12.1.X and 13.0• MAC OS X 10.13
Cluster patching	The cluster patching process now allows you to patch all cluster members without having to first unjoin a replica and re-enroll it after it has been updated. During the cluster patch operation, access request workflow is available so authorized users can request password releases and session access.
Federated login	One Identity Safeguard for Privileged Passwords supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different Identity Provider STS servers and services, such as Microsoft's AD FS.
Immediate recording archival	One Identity Safeguard for Privileged Passwords provides the ability to immediately archive session recordings from a specific Safeguard for Privileged Passwords Appliance to a specified archive target. When an archive server is configured, session recordings are removed from the Safeguard for Privileged Passwords Appliance and stored on the archive server.
Lights Out Management (BMC)	The Lights Out Management feature allows you to remotely manage the power state and serial console to Safeguard for Privileged Passwords using the baseboard management controller (BMC). When a LAN interface is configured, this enables the Appliance Administrator to power on an appliance remotely or to interact with the recovery kiosk.
Multi-request	Authorized Safeguard for Privileged Passwords users can now request multiple password releases or sessions in a single request. In addition, these requests can be saved as a "favorite" access request, providing quick access to the request from the user's Home page.
Safeguard for Privileged Passwords Desktop Player enhancements	The new version of the Safeguard for Privileged Passwords Desktop Player includes the following new features: <ul style="list-style-type: none">• Ability to display user activity as subtitles when playing back a recorded session. The user activity that can be displayed as subtitles includes windows titles, executed commands, mouse activity, and keystrokes, as they occurred during the recorded session.

Feature/Enhancement	Description
	<ul style="list-style-type: none"> • New timeline with user event indicators showing when user activities and screen changes occurred within the recorded session. Clicking an indicator on the timeline takes you to the relevant user event in the recording. • Ability to export the sessions recording file, including the user event subtitles, as a video file.
Security Policy Administrator dashboard	The new Access Request dashboard allows Security Policy Administrators to review and manage access requests from a single location. From this view, the Security Policy Administrator can revoke a request, follow an active session, or terminate a session.
Restore/Suspend accounts	<p>Safeguard for Privileged Passwords allows you to suspend Safeguard for Privileged Passwords managed accounts when they are not in use to reduce the vulnerability of password attacks on privileged accounts.</p> <p>NOTE: This new feature applies to Windows platforms (Windows server and Active Directory accounts) and Unix platforms (AIX, HP-UX, Linux, Solaris, and Mac OS X accounts).</p>
TLS 1.2 Only	To remediate security vulnerabilities identified in early versions of the TLS encryption protocol, Appliance Administrators can configure Safeguard for Privileged Passwords to respond only to TLS 1.2 requests. This allows organizations to comply with the security and strong cryptography requirements in PCI-DSS.
X11 Forwarding	When configuring the settings for SSH session access requests, Security Policy Administrators can now enable Allow X11 Forwarding , which forwards a graphical X-server session from the server to the client.

What's new in version 2.2

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

Table 3: Safeguard for Privileged Passwords 2.2: Features and enhancements

Feature/Enhancement	Description
Additional platform support	Safeguard for Privileged Passwords now supports the management of assets on the following additional platforms:

Feature/Enhancement	Description
	<ul style="list-style-type: none">• FreeBSD• MongoDB• PostgreSQL• RACF - Mainframe LDAP• SAP HANA
Application to Application (A2A) integration	<p>Using the Application to Application service, third-party applications can interact with Safeguard for Privileged Passwords in the following ways:</p> <ul style="list-style-type: none">• Credential retrieval: A third-party application can retrieve a credential from the Safeguard for Privileged Passwords vault in order to perform automated functions on the target asset. In addition, you can replace hard coded passwords in procedures, scripts, and other programs with programmatic calls.• Access request broker: A third-party application can initiate an access request on behalf of an authorized user so that the authorized user can be notified of the available request and log in to Safeguard for Privileged Passwords to retrieve a password or start a session.
Asset administrator dashboard	<p>The Account Automation tab on the Dashboard allows Asset and Directory administrators to view information regarding accounts that are failing different types of tasks, including:</p> <ul style="list-style-type: none">• Accounts where password check tasks failed.• Accounts where password change tasks failed.• Accounts where SSH key change tasks failed.• Accounts where suspend tasks failed.• Accounts where restore tasks failed.
Dynamic grouping and tagging	<p>Dynamic grouping and tagging helps classify assets allowing Safeguard for Privileged Passwords to assign automatically provisioned systems and accounts to a policy.</p> <p>Tags allow Asset administrators to add additional metadata to accounts and assets to enrich the data on the object as it is added to Safeguard for Privileged Passwords. Tags can be dynamically added to assets and accounts based on tagging rules or they can be added manually.</p> <p>Policy administrators can create rules based on tags or from attribute information that is on the account or asset (for</p>

Feature/Enhancement	Description
Event subscription	<p>example, name, platform, partition, network address, and so on) to define group membership.</p> <p>As a Safeguard for Privileged Passwords user, you can now control the email notifications you receive. Using the Manage Email Notifications control in your My Account pane, you can remove the events for which you do not want to receive email notifications.</p> <p>As a Safeguard for Privileged Passwords administrator, you can use the API to subscribe to the events for which you are interested in receiving notifications.</p>
Audit log archive	<p>Safeguard for Privileged Passwords allows you to define and schedule an audit log management task to rotate audit logs from the Safeguard for Privileged Passwords appliance and archive older audit logs to a designated archive server.</p>
Site awareness and network segmentation	<p>As an Appliance administrator, you can define managed networks (network segments) for your organization so Safeguard for Privileged Passwords can more effectively manage assets and accounts, and service access requests. Managed network information is used for scheduling tasks, such as password change and account discovery, and for session management in a clustered environment to distribute the task load. That is, by using managed networks the load is distributed in such a way that there is minimal cluster traffic and appliances that are closest to the target asset are used to perform the task.</p>
Attribute search	<p>The attribute search functionality in the user interface allows you to limit an object list based on the object attributes. For example, in the Accounts view, you can now filter the accounts list based on whether the specified attribute contains the search string entered.</p>
Starling Join	<p>The newest versions of One Identity's on-premises products offer a mandatory One Identity Hybrid Subscription, which helps you transition to a hybrid environment on your way to the cloud. The subscription enables you to join Safeguard for Privileged Passwords with the One Identity Starling software-as-a-service platform. This gives your organization immediate access to a number of cloud-delivered features and services, which expand the capabilities of Safeguard for Privileged Passwords. When new products and features become available to One Identity Starling, the One Identity Hybrid Subscription allows you to use these immediately for Safeguard for Privileged Passwords to add value to your</p>

Feature/Enhancement	Description
	subscription.
Starling Identity Analytics & Risk Intelligence integration	The Starling Identity Analytics & Risk Intelligence service collects and evaluates information from data sources, such as Safeguard for Privileged Passwords, to provide you with valuable insights into your users and entitlements. When integrated with Safeguard for Privileged Passwords, Starling Identity Analytics & Risk Intelligence allows you to identify Safeguard for Privileged Passwords users and entitlements that are classified as high risk and view the rules and details attributing to that classification.

What's new in version 2.3

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

Table 4: Safeguard for Privileged Passwords 2.3: Features and enhancements

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

What's new in version 2.4

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

Custom platform (770747)

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

- Scripts:
<https://github.com/OneIdentity/SafeguardCustomPlatform>
- Command wiki:

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

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

Authentication options (765396)

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

Safeguard Sessions Appliance join (770739)

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

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

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

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

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

What's new in version 2.5

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

Directory based user discovery (713614 and 761638)

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

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

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

Offline Workflow (782735)

To ensure password consistency and individual accountability for privileged accounts, when an appliance loses consensus in the cluster access requests are disabled. In the event of an extended network partition, the Appliance Administrator can manually place an appliance in Offline Workflow mode to run access request workflow on that appliance in isolation from the rest of the cluster. When the network issues are resolved and connectivity is reestablished, the Appliance Administrator can manually resume online operations to merge audit logs, drop any in flight access requests, and return the appliance to full participation in the cluster.

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

System requirements

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

- The Windows desktop client consists of an end-user view and administrator view.
- The web client is functionally similar to the desktop client end-user view.

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

NOTE: If a Safeguard Sessions Appliance is joined to Safeguard for Privileged Passwords, session recording is handled via Safeguard for Privileged Session.

Desktop client system requirements

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

NOTE: When you install the Windows desktop client, these additional components are installed which are used by the embedded sessions module:

- Safeguard for Privileged Passwords Desktop Player: Used to play back a recorded session.
- Safeguard for Privileged Passwords PuTTY: Used to launch an SSH client if PuTTY is not available on the machine.

Table 5: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6

Component	Requirements
Windows platforms	<p>64-bit editions of:</p> <ul style="list-style-type: none"> • Windows 7 • Windows 8.1 • Windows 10 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 <p>i NOTE: Internet Explorer security must be set to use TLS 1.0 or higher. Ensure the proper "Use TLS" setting is enabled on the Advanced tab of the Internet Options dialog (In Internet Explorer, go to Tools Internet Options Advanced tab).</p> <p>i NOTE: If the appliance setting, TLS 1.2 Only is enabled, (Administrative Tools Settings Appliance Appliance Information), ensure the desktop client also has TLS 1.2 enabled. If the client has an earlier version of TLS enabled, you will be locked out of the client and will not be able to connect to Safeguard for Privileged Passwords.</p>
Safeguard for Privileged Passwords Desktop Player	The sessions player is only supported on 64-bit operating systems.

Web client system requirements

Table 6: Web client requirements

Component	Requirements
Web browsers	<p>Desktop browsers:</p> <ul style="list-style-type: none"> • Google Chrome 66 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or later) <p>Mobile device browsers:</p> <ul style="list-style-type: none"> • Apple Safari iOS 10 (or later)

Component	Requirements
	<ul style="list-style-type: none"> • Google Chrome on Android <p>The web client is implemented for modern web browser technology, using:</p> <ul style="list-style-type: none"> • HTML5 • CSS • JavaScript <p>i NOTE: If your browser lacks these required technologies, then use the desktop client.</p>

Product licensing

One Identity Safeguard for Privileged Passwords is made up of a core set of features, such as the UI and Web Services layers, and a number of modules. The One Identity Safeguard for Privileged Passwords 2000 Appliance ships with the following modules, each requiring a valid license to enable functionality:

- Privileged Passwords
- Privileged Sessions

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

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

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

Installing the One Identity Safeguard for Privileged Passwords desktop client

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

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

[Installing the desktop client](#)

[Starting the desktop client](#)

[Uninstalling the desktop client](#)

Installing the desktop client

NOTE: When you install the Windows desktop client, the following components are also installed:

- Safeguard for Privileged Passwords Desktop Player which is used to replay recorded sessions.
- Safeguard for Privileged Passwords PuTTY which is used to launch the SSH client for SSH session requests.

Installing the Safeguard for Privileged Passwords desktop client application

1. To download the Safeguard for Privileged Passwords desktop client Windows installer .msi file, open a browser and navigate to:
`https://<Appliance IP>/Safeguard.msi`
Save the **Safeguard.msi** file in a location of your choice.
2. Run the MSI package.
3. Select **Next** in the **Welcome** dialog.

4. Accept the **End-User License Agreement** and select **Next**.
5. Select **Install** to begin the installation.
6. Select **Finish** to exit the desktop client setup wizard.

Starting the desktop client

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

To start the desktop client application

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

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

3. On the user login screen, enter your credentials and click **Log in**.
 - User Name: Enter your user or display name. Do not include spaces in the User Name.
 - NOTE:** When using directory account credentials, enter your domain\name.
 - Password: Enter the password associated with the user entered above.
4. If your Safeguard for Privileged Passwords user account requires you to log in with secondary authentication, enter the secure password (or token code) for your authentication service provider account and click **Submit**.

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

Uninstalling the desktop client

To uninstall the desktop client

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

Getting acquainted with the console

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

- Windows desktop client

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

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

NOTE: If a Safeguard Sessions Appliance is joined to Safeguard for Privileged Passwords, session recording is handled via Safeguard for Privileged Session.

Since the functionality of these two user interfaces are similar, this guide only describes the Windows desktop client. The Safeguard for Privileged Passwords desktop client console consists of these main components:

[Toolbar controls](#)

[Navigation pane](#)

Toolbar controls

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

Table 7: Toolbar controls

Control	Description
Console Settings	Configure the desktop client application, including notifications and

Control	Description
	Home page widgets, or view product information, including contact information.
User avatar	Modify personal information, view notifications, or log out of the Safeguard client.

Console Settings

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

Notifications

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

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

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

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

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

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

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

Widgets

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

- Requests
- Approvals
- Reviews

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

About

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

Table 8: About dialog tabs

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

User avatar

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

My Account

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

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

To update your personal information

1. From the toolbar, select your user avatar and choose **My Account**.
2. To change your image, select **Change Photo**.
3. To change your email address or **Contact Information**, type into the appropriate box.
4. To change your user password, click **Change Password**.
5. Click **Done** to close the My Accounts pane.

To manage the notifications you receive

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

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

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

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

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

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

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


Log Out

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


Navigation pane

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

Table 9: Navigation pane options

Page	Description
 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

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

NOTE: You can turn **Requests**, **Approvals**, and **Reviews** widgets on or off in [Console Settings](#).

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

Requester's Home page view

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

For more information, see:

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

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

For more information, see:

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

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

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

Table 10: Favorites pane: Action bar buttons

Button	Description
+ New Favorite	Select this button to create a new favorite request. Clicking this button displays the New Access Request dialog allowing you to select the assets, accounts, type of access, and additional details about the request.
<input checked="" type="checkbox"/>	Select this button to display additional options for managing your favorite requests: <ul style="list-style-type: none">• Request Selected• Color Selected• Remove Selected <p>TIP: Select the check box to the left of a favorite request to use these additional buttons. Selecting the request itself will launch the New Access Request dialog allowing you to edit and submit the request.</p>

To submit a favorite request, click the request or select the check box to the left of a request and select **Request Selected**. The **New Access Request** dialog displays

allowing you to edit your selections or enter a required reason or comment before submitting it.

For more information, see:

- [Creating, editing, or removing a favorite request](#)

Approver's Home page view

Your job is to approve or deny the access requests listed on your Home page. Expand **Approvals** to view the requests awaiting your approval.

For more information, refer to these topics:

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

NOTE: As an "approver" user, unless you are also designated as a requester, you will see no favorites listed.

Reviewer's Home page view

Your job is to review completed access requests listed on your Home page. Expand **Reviews** to view the completed requests requiring your review.

For more information, refer to these topics:

- [Reviewing a completed password release request](#)
- [Reviewing a session request](#)

NOTE: As a "reviewer" user, unless you are also designated as a requester, you will see no favorites listed.

Search box

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

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

Rules for using the search functionality:

- Search strings are not case sensitive.
- Wild cards are not allowed.
- Try using quotes and omitting quotes. As you use the product, you will become familiar with the search requirements for the search fields you frequent. Safeguard may perform a general search (for example, omits quotes) or a literal search (for example, includes quotes). Example scenarios follow:
 - On the Settings pane, search strings must be an exact match because a literal search is performed. Do not add quotes or underlines. For example, from the Settings pane, enter `password rules` to return **Safeguard Access | Password Rules**. If you enter **"password rules"** or **password_rules**, the following message is returned: No matches found.
 - On the Users pane search box:
 - A general search does not return anything if you use quotes because it uses a literal search (searches for the quotes). For example: searching for `"ab_misc2"` returns the message: There is nothing to show here.
 - You can use quotes in an attribute search if there are spaces in the search name. For example, entering the following in the search box **Username: "ab_misc2"** returns: `AB_misc2`.
- When multiple search strings are included, all search criteria must be met in order for an object to be included in the results list.
- When you combine a basic search and an attribute search, the order they are entered into the search box matters. The attribute searches can be in any order, but the basic search must come after the attribute searches.
- In large environments, you will see a result number to tell you how many objects match the criteria; however, only the first 200 objects will be retrieved from the server. When you scroll down the list, more objects will be retrieved (paged) as needed.

To search for accounts

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

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

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

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

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

To conduct an attribute search

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.

The drop-down menu lists a limited number of attributes that can be searched; however, you can perform an attribute search using the English name of any attribute as it appears in

the API. Nested attributes can be chained together using a period (.). To see a list of all the attributes, see the API documentation. For information about the API, see [How do I access the API](#).

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

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

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

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

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

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

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

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

Privileged access requests

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

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

As a Safeguard for Privileged Passwords user, your **Home** page provides a quick view to the access request tasks that need your immediate attention. In addition, Safeguard for Privileged Passwords can be configured to alert you when you have pending tasks awaiting your attention. For more information, see [Configuring alerts](#) on page 32.

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

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

Requesters can also define favorite requests, which then appear on their **Home** page for subsequent use. For more information, see [Creating, editing, or removing a favorite request](#) on page 30.

- Designated "approvers" see tasks related to approving (or denying) and revoking access requests.
- Designated "reviewers" see tasks related to reviewing completed (checked in) access requests, including playing back a session if session recording is enabled.

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

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

Creating, editing, or removing a favorite request

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

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

To create a favorite request from your Home page

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

Click **Add**.

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

To create a favorite request from the New Access Request dialog

1. At the bottom of the **New Access Request** dialog, click the **Add to Favorites** button when you are creating a new request. The **Add to Favorites** button is enabled when you have selected the minimum required information (that is, at least

one asset, account, and an access type) for the access request.

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

To change a favorite request's icon color

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

To remove a favorite request

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

Configuring alerts

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

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

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

Table 11: Notification types

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

Toast notifications

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

To enable toast notifications

1. Open  [Console Settings](#).
2. Select the **Enable Toast Notifications** check box.

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

Email notifications

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

- You must set your email address correctly in **My Accounts**. For more information, see [User avatar](#) on page 23.
- Contact your Security Policy Administrator to ensure the access request policies are configured to notify people of pending access workflow events.
- Contact your Appliance Administrator to ensure the SMTP server is configured for email notifications.

Password release request workflow

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

Typically a password release request follows this workflow.

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

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

Requesting a password release

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

- ① **NOTE:** You can configure One Identity Safeguard for Privileged Passwords to notify you of pending password release workflow events, such as when a password release request is pending, denied or revoked, and so forth. For more information, see [Configuring alerts](#) on page 32.

To request a password release

1. From your **Home** page, click **New Request** to open the **New Access Request** dialog.
 - NOTE:** You can also submit an access request from your **Favorites** pane, if you previously saved it as a favorite.
2. On the **Asset Selection** tab, select the assets to be included in the access request.

Limit: 50 assets

The assets available for selection are based on the scope defined in the entitlement's access request policies.
3. On the **Account & Access Type** tab, select the accounts to be included in the access request and the type of access being requested for each selected account.
 - **Account:** The available account appears in the **Account** column. When an asset has multiple accounts available, either **Select Account(s)** or the account name appears as a hyperlink in the **Account** column. Click the hyperlink in the **Account** column to display a list of accounts available and select the accounts to be included in the access request.
 - **Access Type:** The type of access request appears in the **Access Type** column. When multiple access request types are available, this value appears as a hyperlink, which when selected displays an additional dialog allowing you to select the access type. Select **Password Request**.

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

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

allows you to set the days, hours, and minutes that you want the password and overrides the checkout duration set in the access request policy.

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

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

When multiple accounts are specified in the request, if any of the selected accounts require a ticket number, you must specify a valid ticket number. The specified ticket number will be applied to all of the requests associated with this access request.

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

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

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

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

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

Limit: 255 characters

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

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

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

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

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

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

Taking action on a password release request

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

To take action on a password release request

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

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

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

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

State	Description
All	Requests in all states.
Available	Approved requests that are ready to view or copy.
Approved	Requests that have been approved, but the checkout time has not arrived.
Pending	Requests that are waiting for approval or for pending accounts restored when using the Safeguard for Privileged Passwords suspend feature.
Revoked	Approved requests retracted by the approver. The approver can revoke a request between the time the requester views the password and checks it in.
Expired	Requests for which the checkout duration has elapsed.
Denied	Requests denied by the approver.

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

3. Select an account to see the details of the password release request.
4. Take the following actions on password release requests:

State	Actions
Available	Select ☐ Copy to checkout the password. This puts the password into your copy buffer, ready for you to use.

State	Actions
	<p>Select <input checked="" type="checkbox"/> Check-In to complete the password checkout process.</p> <p>Select Show Password to view the password on your screen. The password displays on your screen for 20 seconds.</p> <p>Selecting either Copy or Show Password constitute a password "checkout".</p> <p>If the password changes while you have it checked out, and your current request is still valid, select either Copy or Show Password again to obtain the new password.</p> <p>Select Hide Password to conceal the password from view.</p>
Approved	<p>Select <input checked="" type="checkbox"/> Cancel to remove the request.</p> <p>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.</p>
Pending	<p>Select <input checked="" type="checkbox"/> Cancel to remove the request.</p>
Revoked	<p>Select <input type="checkbox"/> Resubmit Request to request the password again.</p> <p>Select <input type="checkbox"/> Remove to delete the request from the list.</p>
Expired	<p>Select <input type="checkbox"/> Remove to delete the request from the list.</p>
Denied	<p>Select <input type="checkbox"/> Resubmit Request to request the password again.</p> <p>Select <input type="checkbox"/> Remove to delete the request from the list.</p>

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.

NOTE: You can configure Safeguard for Privileged Passwords to notify you of a password release request that requires your approval. For more information, see [Configuring alerts](#) on page 32.

To approve or deny a password release request

1. From your **Home** page, the **Approvals** widget has these controls:

- a. Select **▼ (expand down)** to open the list of approvals.
- b. Select **☐ Popout** to float the **Approvals** pane.

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

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

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

State	Description
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.

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

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

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

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

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

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 32.

To review a completed password release request

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

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

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

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

Session request workflow

With the embedded sessions module, authorized users can authorize connections, view active connections, limit access to specific resources, be alerted if connections exceed pre-set time limits and even terminate connections.

Typically a session request follows this workflow.

1. **Request:** Users that are designated as an authorized "user" of an entitlement can request an RDP or SSH 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 Safeguard for Privileged Passwords Player to replay the session as part of the review process.

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

About sessions and recordings

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

Important notes

- The Safeguard for Privileged Passwords Desktop Player, used to play back recorded sessions, is installed with the Windows desktop client.
- Safeguard for Privileged Passwords PuTTY is installed with the Windows desktop client and is used to launch the SSH client if PuTTY is not available on the machine.
- For some systems (SUSE and some Debian systems) that use SSH, you must enable password authentication in the package generated configuration file (sshd_config). For example, in the debian sshd_config file, set the following parameter: PasswordAuthentication yes.
- Sessions requests are enabled by default. However, if authorized users cannot request sessions, check the **Session Requests Enabled** setting (**Administrative Tools | Settings | Access Request | Enable or Disable Services**).
 - ① **NOTE:** You must have Appliance Administrator permissions to manage the service settings.
- All session activity - every packet sent and action that takes place on the screen, including mouse movements, clicks and keystrokes - is recorded and available for play back.
- If Safeguard for Privileged Passwords detects no activity for 10 minutes during a privileged session, the session is terminated.

Requesting session access

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

You can configure One Identity Safeguard for Privileged Passwords to notify you of pending access request workflow events, such as when a session request is pending, denied or revoked, and so forth. For more information, see [Configuring alerts](#) on page 32..

To request session access

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

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

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

Limit: 50 assets

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

3. On the **Account & Access Type** tab, select the accounts to be included in the access request and the type of access being requested for each selected account.

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

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

- If **None** is selected in the access request policy, the accounts Safeguard for Privileged Passwords retrieved from the vault will be available for selection. The selected account will then be used when the session is requested.
- If **User Supplied** is selected in the access request policy, you will be required to enter the user credentials as part of the request workflow, prior to launching the SSH or RDP session.
- If **Linked Account** is selected in the access request policy, linked directory accounts will be available for selection. The selected account will then be used when the session is requested.
- If **Directory Account** is selected in the access request policy, only the

specified directory accounts will be available for selection. The selected directory account will then be used when the session is requested.

- **Access Type:** The type of access request appears in the **Access Type** column. When multiple access request types are available, this value appears as a hyperlink, which when selected displays an additional dialog allowing you to select the access type. Select one of the following for a session request: **RDP** or **SSH**.

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

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

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

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

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

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

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

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

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

Limit: 255 characters

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

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

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

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

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

Taking action on a session request

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

To take action on a session request

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

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

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

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








State	Description
All	Requests in all states.
Available	Approved requests that are ready (that is, a session that can

State	Description
	be launched).
Approved	Requests that have been approved, but the checkout time has not arrived.
Pending	Requests that are waiting for approval.
Revoked	Approved requests retracted by the approver. The approver can revoke a request between the time the requester launches the session and checks it back in. When a user with Security Policy administrator permissions revokes a "live" session, the active session is terminated.
Expired	Requests for which the checkout duration has elapsed.
Denied	Requests denied by the approver.

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

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

State	Actions
Available	<p>Click ► Launch to launch the SSH client or Remote Desktop Connection. For more information, see Launching the SSH client or Launching an RDP session.</p> <p>Click ✓ Check-In to complete the checkout process once you have ended your session.</p> <p>In addition, you can use the following buttons to view or copy information into the configuration dialog that contains the credentials needed to launch the session:</p> <ul style="list-style-type: none"> • View: Click this button to view the password or connection string, which is required to launch the session. • Copy: Click this button to copy a value to the copy buffer. • Help: Click this button to copy the value into the appropriate field of the configuration dialog. <p>1 NOTE: The configuration dialogs are populated with the required information; these actions are available if the fields are not populated for some reason.</p>




State	Actions
Approved	Click  Cancel to remove the request. A sessions request changes from "Approved" to "Available" when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
Pending	Click  Cancel to remove the request.
Revoked	Click  Resubmit Request to request the session again. Click  Remove to delete the request from the list.
Expired	Click  Remove to delete the request from the list.
Denied	Click  Resubmit Request to request the session again. Click  Remove to delete the request from the list.



Approving a session request

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

You can configure Safeguard for Privileged Passwords to notify you of an access request that requires your approval. For more information, see [Configuring alerts](#) on page 32..

To approve or deny a sessions request

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



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

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

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

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

- 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 Approve or Deny a sessions request. Optionally, enter a comment of up to 255 characters.
Pending Additional Approvers	Select  to Deny a sessions request. Optionally, enter a comment of up to 255 characters.
Approved	Select  to Deny or Revoke an approved request. You can revoke a request between the time the requester views it and checks it in. Any eligible approver can deny an access request after it has already been approved or auto-approved. Once disallowed, the requester will no longer be able to access the requested session, but he is given another opportunity to request that session again. The requester receives an email notifying him that the request was denied. For more information, see Configuring alerts on page 32.

Launching the SSH client

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

To launch the SSH client to begin your session

- 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.
- Click the ► **Launch** button to the right of the asset name. Clicking this button displays the **PuTTY Configuration** dialog. The required information is populated, click **Open** to launch the SSH client.

- NOTE:** If the required information is not populated in the **PuTTY Configuration** dialog, use the following buttons to copy and paste the information into the dialog:
- a. Use the buttons to the right of the **Hostname Connection String** to perform the following tasks:
 - **View:** To view the hostname connection string.
 - **Copy:** To copy the value to your copy buffer, which can then be pasted into the Hostname field of the **PuTTY Configuration** dialog.
 - **Help:** To copy the value into the Hostname field of the PuTTY Configuration dialog.
 - b. Use the buttons to the right of the **Password** to perform the following tasks:
 - **View:** To view the password.
 - **Copy:** To copy the password to your copy buffer, which can then be pasted into the Password field of the **PuTTY Configuration** dialog.
 - **Help:** To copy the value into the Password field of the **PuTTY Configuration** dialog.
 - NOTE:** The Password field only appears if the **Include password release with session requests** option (Access Config tab) is selected in the entitlement's access request policy.

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

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

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

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

Launching an RDP session

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

To launch a remote desktop connection to begin your RDP session

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

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

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

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

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

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

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

This makes the session request available to reviewers. If the **Record Sessions** option is enabled in the policy, the reviewer can playback 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 32..

To review a completed sessions request

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

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

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

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

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

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

To play back a session (Request Workflow dialog)

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

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

2. Locate an Initialize Session event and click **▶ Play** to launch the Safeguard for Privileged Passwords Desktop Player.

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

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

3. Accept the certificate to continue.

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

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

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

For more information about the Safeguard for Privileged Passwords Desktop Player and navigating through a recording, see [Recording navigation](#).

Safeguard Desktop Player

The Safeguard for Privileged Passwords Desktop Player is installed with the Windows desktop client. When the player is launched from the desktop client, the recording is being streamed from the Safeguard appliance. It only exists on the disk for the lifetime of the player session. That is, when you shut down the player, the recording file is removed from the cache.

When you launch the Safeguard for Privileged Passwords Desktop Player, the main view displays, which consists of the following tabbed pages:

- Information: Displays detailed information about the recorded session and allows you to play back the recording.
- Warnings: Displays warnings associated with the recording.

Information tab

The information tab displays the following details for the session recording.

Table 12: Safeguard Desktop Player: Information tab

Control	Description
Session recording location	Displays the path of where the recording is currently stored.
Thumbnail	<p>Click the thumbnail in the right corner of the screen to play back the recording.</p> <p>i NOTE: The thumbnail is only available for RDP Drawing and SSH Session Shell channels.</p> <p>i NOTE: A blinking red recording button in the upper right corner of the thumbnail indicates that the session is "live" allowing you watch the session in follow mode. Follow mode is only available to users with Security Policy Administrator permissions.</p>
Validation	The Safeguard for Privileged Passwords Desktop Player checks the

Control	Description
indicators	<p>upstream and downstream traffic from the recording and validates the digital signature and timestamp. The indicators across the top of the screen show the results of this validation process, where all indicators should display a green check mark.</p> <p>If the Signature or Timestamp indicators are red Xs, this indicates that the corresponding certificate has not been validated. Contact your Appliance Administrator.</p>
Recording details	<p>Displays details about the recording, such as:</p> <ul style="list-style-type: none"> • Date • Duration • File size • Session ID
User	Displays the name of the user that authenticated to the remote machine..
Connections	Displays connection information, including the address and port of client computer and the remote machine.
Channels	<p>The Channels pane displays the different types of data streams available for a recorded session.</p> <p>An SSH session recording will contain a single channel. Valid channels for an SSH session recording are:</p> <ul style="list-style-type: none"> • Session Shell: This is the only SSH channel that can be played back using the desktop player and it contains the actions performed during the session. • Session SFTP: Contains data that was transferred using the Secure File Transfer protocol (SFTP). Since this is a file transfer protocol, there is no recording file available for play back. <ul style="list-style-type: none"> • NOTE: This channel is only available when Allow SFTP is selected on the Sessions Settings tab in an access request policy. • Session SCP: Contains data that was transferred using the Secure Copy protocol (SCP). Since this is a file transfer protocol, there is no recording file available for play back. <ul style="list-style-type: none"> • NOTE: This channel is only available when Allow SCP is selected on the Sessions Settings tab in an access request policy. • X11: Use this channel to play back the graphical X-server session that was forwarded from the server to the client.

Control	Description
	<p>NOTE: This channel is only available when Allow X11 Following is selected on the Sessions Settings tab in an access request policy.</p> <p>An RDP session may contain multiple channels. Valid channels for an RDP session recording are:</p> <ul style="list-style-type: none"> • Clipboard: Contains any data that was transferred through the clipboard; there is no recording file available for play back. <p>NOTE: This channel is only available when Allow Clipboard is selected on the Session Settings tab in an access request policy.</p> <ul style="list-style-type: none"> • Drawing: All RDP sessions will have a Drawing channel, which contains the actions taken during the session. This type of channel is most likely to be replayed. • Sound: Contains any audio associated with the recording. <p>Click the ► Play button next to the channel to play back the session recording.</p> <p>Clicking the expansion button next to a channel displays a list of key details.</p>

Warning tab






The warning tab displays any warnings encountered when opening and processing the recording.

Toolbar

Use the toolbar buttons located at the top of the main view as described below.

Table 13: Safeguard Desktop Player toolbar

Option	Description
← Back	<p>Displays the previous view. For example, if you clicked play and are in the video view, clicking this button returns you to the recording information view.</p> <p>NOTE: When no recording is loaded, there is an additional view that prompts you to drag and drop a recording file onto the player. Once you add the recording file, the recording information view displays.</p>
► Play Channel	Plays back the selected sessions recording.

Option	Description
	<p> NOTE: This button is disabled in follow mode.</p> <p> NOTE: For more information on navigating the video view, see Recording navigation.</p>
 Export Video	<p>Exports the sessions recording file as a video file (WEBM format).</p> <p> NOTE: To play back the WEBM video, use any standard video player, such as the one available with Firefox or Google Chrome.</p>
 Settings	<p>Allows you to import keys and certificates, access the One Identity support web site for help, and view version information about the player.</p>




Recording navigation




Once the play back window opens you can use the controls at the bottom of the screen or keyboard shortcuts to navigate through the recording.

Recording navigation controls

Use the controls at the bottom of the screen to navigate through the sessions recording.

Table 14: Navigation controls: Playback mode

Control	Action
Timeline	<p>Shows you where you are within the recording. The timeline can also show indicators for user events that occurred during a recorded session. Clicking an indicator on the timeline takes you to the relevant user event in the recording.</p> <p>For more information on showing or hiding the user event indicators on the timeline, see Configure seeker indicators below.</p>
Play speed	Allows you to increase or decrease the replay speed.
 Skip back	Allows you to jump back to the previous user event in the recording.
 Play	Play allows you to play the recording.
 Pause	Pause allows you pause the recording.

Control	Action
 Skip forward	Allows you to jump forward to the next user event in the recording.
 Closed Captioning	<p>Allows you to display subtitles for the video that list user events as they occurred within the recorded session.</p> <p>User events that may appear as subtitles include windows titles, executed commands, mouse activity, and keystrokes.</p>
 Configure seeker indicators	<p>Allows you to configure the visibility of user event indicators on the timeline. To show a user event indicator move the toggle to the right; to hide a user event indicator move the toggle to the left.</p> <p>NOTE: The type of user events that can be included in the timeline depends on the type of session:</p> <ul style="list-style-type: none"> • RDP: Windows titles, keystrokes, mouse activity, and on-screen changes • SSH: Commands, keystrokes, and on-screen changes
Scaled video	<p>Allows you to view the recording in a smaller or larger window. Clear this check box to play the video using the original resolution.</p> <p>NOTE: The video is rendered at the same resolution as the original session. This setting adjusts the video size based on the size of the viewing screen.</p>

When you are watching a "live" session, the playback navigation controls are replaced with different follow mode navigation controls.

NOTE: Follow mode is only available to users with Security Policy administrator permissions.

Table 15: Navigation controls: Follow mode

Control	Action
Terminate	Allows you to end the current session you are following.
Live	Indicates you are following a "live" session.


Keyboard shortcuts

You can also use the following shortcut keys to navigate through the recording.


Table 16: Keyboard shortcuts: Playback mode

Shortcut keys	Action
SPACE	Play/pause recording
Ctrl+Z	Enable video scaling
f	Toggle full screen replay
[Decrease replay speed
]	Increase replay speed
=	Reset replay speed
Shift + Left Arrow	Jump backwards - short
Alt + Left Arrow	Jump backwards - medium
Ctrl + Left Arrow	Jump backwards - long
Shift + Right Arrow	Jump forward - short
Alt + Right Arrow	Jump forward - medium
Ctrl + Right Arrow	Jump forward - long

Exporting video

Use the  **Export Video** button at the top of the Safeguard Desktop Player to export the sessions recording file as a video file (WEBM format). This WEBM file can then be played back using any standard video player, such as the one available with Firefox or Google Chrome.

To export a video

1. In the Safeguard for Privileged Passwords Desktop Player, click  **Export Video**.
The Export screen appears, displaying the name of the video file and the size of the file.
2. If you want to include user event subtitles with the exported file, select the **Subtitle** check box in the upper left corner of the screen.
3. Click the browse button (""") in the lower right corner of the screen to specify the location where the file is to be stored.

The specified location appears in the **Export to** field.

4. Click the **Export** button.

An Export Successful message appears.

Key descriptions

Expanding a channel in the **Channels** pane of the Safeguard for Privileged Passwords Desktop Player displays additional details about the recording. The keys displayed depends on the type of channel selected. The keys marked with an asterisk (*) may provide you some additional insight into the recording; most of the other keys are internal values.

Table 17: Safeguard Desktop Player: Key descriptions

Key	Description
auth_method	Authentication method used.
bpp	Color depth (bits-per-pixel) of the remote machine.
channel_id	Internal identifier assigned to the channel being recorded.
channel_name	Internal name assigned to the channel being recorded.
channel_policy	Internal name assigned to the channel policy being used.
channel_type	Type of channel: SSH or RDP
client_address*	Address of the client computer.
client_address.ip	IP address of the client computer.
client_address.port	Port used by the client computer.
client_id	Internal identifier assigned to the client computer.
client_x509_subject	Client certificate subject.
connection	Internal connection policy being used.
connection_id	Internal connection identifier assigned to the recording.
data_received	Data received flag: True
data_sent	Data sent flag: True
dst_ip	IP address of the session recording module.
duration*	Duration of the recording.
duration_raw	Raw duration of the recording (should be the same as the duration).
exit_status	Exit status of the program run on the remote server.

Key	Description
height_rows*	Number of rows shown in the SSH terminal.
initiator	Who initiated the connection: Client
is_processable	Indicates if the session can be processed: True
local_ip	IP address of the sessions module.
protocol*	Protocol used: SSH or RDP
remote_username*	Name of the user name that log into the remote machine.
server_address*	Address and port of the remote machine.
server_address.ip	IP address of the remote machine.
server_address.port	Port used to connect to the remote machine.
server_id	Internal identifier assigned to the remote machine.
server_ip	IP address of the remote machine.
session_end	Time (in milliseconds) when the session ended.
session_id	Internal session ID assigned to the session.
session_start	Time (in milliseconds) when the session started.
Signature	Validity of the Session Recording Signing certificate.
source	Source protocol: SSH or RDP
stream_type	Internal type assigned to the recording stream.
term	Type of SSH terminal.
Timestamp	Validity of the Timestamping Authority certificate.
username	Name of the user that authenticated to the remote machine.
width_cols	Width (in columns) of the original SSH session screen.
width_pix*	Width (in pixels) of the original SSH session screen.
width*	Screen width of the RDP session.

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

Contacting us

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

Technical support resources

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

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

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

A

- access request workflow 29
- approve password release request 38
- approve session access request 45
- authentication options 14

C

- cancel pending session access request 45
- Clipboard channel 52
- configure alerts 32
- contact information
 - change personal information 23
- continued access workflow 15
- custom platform 13

D

- desktop client
 - application settings 22
 - install 19
 - start 20
 - system requirements 16
 - uninstall 20
- directory based user discovery 15
- disable
 - toast notifications 32
- Drawing channel 52

E

- email
 - configure Safeguard to receive notifications 33
- enable
 - toast notifications 22, 32
- export
 - video 56

F

- favorites
 - create 30
 - remove 31
 - set color 31
- forced access request 15

H

- Home page
 - about 24
 - navigation pane 24
 - widgets 25

I

- install
 - desktop client 19

J

join Safeguard for Privileged Passwords to Safeguard Sessions Appliance 14

L

launch
 RDP session 47
 Safeguard Desktop Player 50
 SSH client 46
licensing 18

N

navigation
 recording 54

P

password
 change 23
password release
 check-in 37
 checkout 36
password release request 33
 approval 38
 cancel pending request 37
 check-in 36
 checkout 36
 remove request 37
 resubmit request 37
 review 39
 workflow 33
photo
 change 23

play back recorded session 50
product licensing 18

R

RDP session
 launch 47
recording navigation 54
remove
 session access request 45
replay recorded session 50
request password release 33
request workflow
 dialog 50
 password release requests 33
review
 password release request 39
 session access request 49
run in the system tray 22

S

Safeguard
 features 6
 new features in 2.1.0 8
 new features in 2.2 10
 new features in 2.3 13
 new features in 2.4 13-14
Safeguard Desktop Player
 channels 52
 export video 56
 key descriptions 57
 navigation 54
search box
 using 27

- secondary authentication
 - login 20
- session access request 41
 - approve 45
 - cancel pending request 45
 - check-in session 43
 - launch RDP session 47
 - launch session 43
 - launch SSH client 46
 - remove 45
 - resubmit request 45
 - review 49
 - revoke 46
- session recording
 - about 40
 - navigation controls 54
 - play back 50
- session request workflow 39
- Session SCP channel 52
- Session SFTP channel 52
- Session shell channel 52
- sessions
 - about 40
- sessions appliance join 14
- settings
 - desktop client application settings 22
 - run in the system tray 22
- Sound channel 52
- SSH session
 - launch SSH client 46
- start desktop client 20
- system requirements 16
 - desktop client 16
 - web client 17

T

- toast notifications 32
 - about 22
- toolbar
 - main screen 21

U

- uninstall desktop client 20
- user
 - change password 23
 - change personal contact information 23
 - change photo 23

W

- web client
 - about 21
 - system requirements 17
- widgets
 - approvals widget, controls 38, 45
 - requests widget, controls 36, 43
 - reviews widget, controls 39, 49