One Identity Safeguard 2.1

User Guide

Legend

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

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

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

Safeguard User Guide
Updated - December 2017
Version - 2.1

Contents

1

Introduction

The One Identity Safeguard 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 desktop client.

Introduction to One Identity Safeguard

The One Identity Safeguard Appliance is built specifically for use only with the Safeguard 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 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 Safeguard for Privileged Sessions** allows you to issue privileged access for a specific period or session to administrators, remote vendors and high-risk users with full recording and replay. With this ability, you can easily meet your auditing and compliance demands. In addition, Safeguard for Privileged Sessions serves as a proxy to ensure your critical assets are protected from any malicious software that might be lurking on an administrator's machine. It provides a single point of control from which you can authorize connections, limit access to specific resources, view active connections, record all activity, and terminate connections. Safeguard for Privileged Sessions is a critical component of the One Identity

privileged access management products and is deployed on the same hardened secure appliance as Safeguard for Privileged Passwords.

Key features

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

Table 1: One Identity Safeguard 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 appliances can be clustered to ensure high availability. Passwords and sessions can be requested from any appliance in a Safeguard cluster. This distributed clustering design also enables the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster.
RESTful API	Safeguard 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.
Activity Center	Using the Activity Center, you can quickly and easily view all actions executed by Safeguard 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.

Feature	Description
Two-factor authentication support	Protecting access to passwords with another password isn't enough. Enhanced security by requiring two-factor authentication to Safeguard. Safeguard supports any RADIUS-based 2FA solution and One Identity's Starling Two-Factor Authentication service.
Smartcard support	Authentication of your privileged users can be integrated with Microsoft's Active Directory support for Smartcards or manually uploaded to the Safeguard appliance itself.
Full session audit, recording and replay	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.
Proxy access	Safeguard for Privileged Sessions 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. Safeguard for Privileged Sessions can proxy and record Unix/Linux, Windows, network devices, firewalls, routers and more.
Work the way you want	Safeguard for Privileged Sessions enables administrators to choose their access tools and tool preferences (for example, PuTTY) when gaining access to privileged sessions. This creates a frictionless solution that gives administrators the access they need while meeting compliance and security regulations.
Command detection	During a privileged session, Safeguard 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). NOTE: For an RDP session, Safeguard can detect the title of any window that is opened on the desktop during a privileged session.
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	Safeguard for Privileged Sessions provides full support for the SSH and RDP protocols. In addition, administrators can decide

Feature	Description
	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 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 One Identity Safeguard 2.1

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

Table 2: New features and enhancements

Feature/Enhancement	Description
Additional platform support	Safeguard now supports the management of assets on the following additional platforms: • ACF2 - Mainframe r14 and r15 • ACF2 - Mainframe LDAP r14 and r15 • Debian GNU/Linux 9 • ESXi 6.5 • Fedora 26 • Fortinet FortiOS 5.2 and 5.6 • F5 Big-IP 12.1.X and 13.0 • MAC OS X 10.13
Cluster patching	The cluster patching process now allows you to patch all cluster members without having to first unjoin a replica and re-enroll it after it has been updated. During the cluster patch operation, access request workflow is available so authorized users can request password releases and session access.
Federated login	One Identity Safeguard supports the SAML 2.0 Web Browser SSO Profile, allowing you to configure federated authentication with many different Identity Provider STS (IdP-STS) servers and services, such as Microsoft's AD FS and Azure AD.
Immediate recording archival	One Identity Safeguard provides the ability to immediately archive session recordings from a specific Safeguard appliance to a specified archive target. When an archive server is configured, session recordings are removed from the Safeguard appliance and stored on the archive server.

Feature/Enhancement	Description
Lights Out Management (BMC)	The Lights Out Management feature allows you to remotely manage the power state and serial console to Safeguard 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 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 Desktop Player enhancements	The new version of the Safeguard Desktop Player includes the following new features: • Ability to display user activity as subtiltes when playing back a recorded session. The user activity that can be displayed as subtitles includes windows titles, executed commands, mouse activity, and keystrokes, as they occurred during the recorded session. • New timeline with user event indicators showing when user activities and screen changes occurred within the recorded session. Clicking an indicator on the timeline takes you to the relevant user event in the recording. • Ability to export the sessions recording file, including the user event subtitles, as a video file.
Security Policy Administrator dashboard	The new Access Request dashboard allows Security Policy Administrators to review and manage access requests from a single location. From this view, the Security Policy Administrator can revoke a request, follow an active session, or terminate a session.
Restore/Suspend accounts	Safeguard allows you to suspend Safeguard managed accounts when they are not in use to reduce the vulnerability of password attacks on privileged accounts. NOTE: This new feature applies to Windows platforms (Windows server and Active Directory accounts) and Unix platforms (AIX, HP-UX, Linux, Solaris, and Mac OS X accounts).
TLS 1.2 Only	To remediate security vulnerabilities identified in early versions of the TLS encryption protocol, Appliance Administrators can configure Safeguard to respond only to TLS 1.2 requests. This allows organizations to comply with the

Feature/Enhancement	Description
	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.

2

System requirements

One Identity Safeguard 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.

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.

NOTE: When you install the Windows desktop client, these additional components are installed which are used by the One Identity Safeguard for Privileged Sessions module:

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

Table 3: Desktop client requirements

Component	Requirements
Technology	Microsoft .NET Framework 4.6
Windows platforms	32-bit or 64-bit editions of: • Windows 7 • Windows 8.1

Component	Requirements
	• Windows 10 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 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). NOTE: If the appliance setting, **TLS 1.2 Only** is enabled, (**Administration Tasks** | **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.
Safeguard Desktop Player	The sessions player is only supported on 64-bit operating systems.

Web client system requirements

Table 4: Web client requirements

Component	Requirements
Web browsers	Desktop browsers: • Google Chrome 58 (or later) • Microsoft Internet Explorer 11 and Edge • Mozilla Firefox 52 (or later) Mobile device browsers: • Apple Safari iOS 8 (or later) • Google Chrome on Android The web client is implemented for modern web browser technology, using: • HTML5 • CSS

Component	Requirements
	• JavaScript NOTE: If your browser lacks these required technologies, then use the desktop client.

Product licensing

One Identity Safeguard 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 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 module to operate. More specifically, if any module is installed, Safeguard 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 user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

3

Installing the One Identity Safeguard 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 desktop client application:

Installing the desktop client

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

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

To install the Safeguard desktop client application

1. To download the Safeguard 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 2000 appliance has been configured and licensed. As a Safeguard user, if you get an "appliance is unlicensed" notification, contact your Appliance Administrator.

To start the desktop client application

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

   NOTE: When entering an IPv6 address, enclose the IPv6 address in square brackets.
3. On the user log-in screen, enter your credentials and click (or tap) **Log in**.
   - User Name: Enter your user or display 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 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 (or tap) **Submit**.

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

Getting acquainted with the console

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

The Safeguard desktop client console consists of these main components:

Toolbar

The Toolbar along the top-right corner of the Safeguard console, has these controls:

Table 5: Toolbar controls

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

Settings

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

Notifications

Use the following options to control notifications within Safeguard:

- **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.

Widgets

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

- Requests
- Approvals
- Reviews

When you enable the widgets, the corresponding controls display on your **Home** page.

Reset Notifications: Click (or tap) this button to re-enable any notifications pop ups that have been preciously suppressed.

About

Click (or tap) the **About Safeguard** link, to display the following information:

Table 6: About dialog tabs

Tab	Description
About	The trademark and copyright information.
Contact	Information about how to get in touch with One Identity.

Tab	Description
Components	A list of third-party components used in Safeguard.
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 (or tap) the user avatar (or the Welcome link with your user name) to modify your personal information, view notifications, or log out of Safeguard.

My Account

Click (or tap) **My Account** to modify your personal information.

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 (or tap) **Change Password**.

Notifications

Notifications indicates the number of message awaiting your attention. Click (or tap) **Notifications** to display the **Home** page and notifications that are awaiting your attention.

Log Out

Click (or tap) **Log Out** to log out of the Safeguard desktop client.

Navigation pane

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

Table 7: 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, 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 Settings.

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

Requester's Home page view

Click (or tap) 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 action bar buttons at the top of the Favorites pane to manage your favorite requests.

Table 8: Favorites pane: Action bar buttons

Button	Description
+ New Favorite	Select this button to create a new favorite request. Clicking this button launches the New Access Request dialog allowing you to select the assets, accounts, type of access, and additional details about the request.
☑	Select this button to display additional options for managing your favorite requests: • Request Selected • Color Selected • Remove Selected TIP: Select the check box to the left of a favorite request to use these additional buttons. Selecting the request itself will launch the New Access Request dialog allowing you to edit and submit the request.

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 appears 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

To search for accounts

1. Enter a text string in the **Search** box. As you type, the list displays item names that contain the string.

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

   NOTE: The text search is not case sensitive and does not allow wild cards.

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

2. To clear search criteria, click (or tap) **Clear** to delete the text string.

Privileged access requests

One Identity Safeguard 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/or 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 user, your **Home** page provides a quick view to the access request tasks that need your immediate attention. In addition, Safeguard can be configured to alert you when you have pending tasks awaiting your attention. For more information, see Configuring alerts on page 25.

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 23.
- 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 allows you to add an access request as a **Favorite** to your **Home** page.

NOTE: **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 (or tap) **+ New Favorite**.
2. On 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 (or tap) **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 (or tap) this hyperlink to select the access type.
3. Select the **Add to Favorites** button .
4. On the Add to Favorites dialog,
    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 (or tap) **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, select the **Add to Favorites** button when you are creating a new request.

   NOTE: 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. On the Add to Favorites dialog,

   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.

   Click (or tap) **Add**.

To change a favorite request's icon color

1. At the top of the **Favorites** pane, click (or tap) the ☑ button to display the **Color Selected** button.
2. Select the check box of the left of the favorite request to be changed.

   NOTE: Selecting a favorite request, instead of the check box, launches the New Access Request dialog to edit and submit the access request.

3. Click (or tap) **Color Selected**.
4. On 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 (or tap) the ☑ button to display the **Remove Selected** button.
2. Select the check box to the left of the favorite request to be removed.

   NOTE: Selecting a favorite request, instead of the check box, launches the New Access Request dialog to edit and submit the access request.

3. Click (or tap) the **Remove Selected** button.
4. Select **Yes** to confirm.

Configuring alerts

The requester, approver, and reviewer of access requests receive event notifications based on the condition that the password for the request is checked out for that requester. The following email notifications can be sent:

- Requester
  - Access Request Approved
  - Access Request Denied
  - Access Request Revoked
  - Access Request Expired
- Approver
  - Access Request Pending Approval
- Reviewer
  - Access Request Pending Review

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

Table 9: 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 desktop client.

To enable toast notifications

1. Open Settings.
2. Select the **Enable Toast Notifications** option.

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.

Email notifications

You must configure One Identity Safeguard 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 18.
- 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 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 users, or be auto-approved. This process ensures the security of account passwords, provides accountability, and provides dual control over the system accounts.
3. **Review**: The Security Policy Administrator can optionally configure an access request policy to require a review of completed password release requests for accounts in the scope of the policy.

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

Requesting a password release

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

NOTE: You can configure One Identity Safeguard 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 25.

To request a password release

1. From your **Home** page, click (or tap) **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.

   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 (or tap) 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 launches 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 (or tap) the **— Delete** action bar 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 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 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 (or tap) the **Add to Favorites** button.

   The Add to Favorites dialog appears 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 launches 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 (or tap) **Submit Request**.

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

Taking action on a password release request

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

To take action on a password release request

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

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

2. Open the list of requests and select one of 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.
Revoked	Approved requests retracted by the approver. NOTE: 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. • Select **Check-In** to complete the password checkout process. • Select **Show Password** to view the password on your screen. The password displays on your screen for 20 seconds.

State	Actions
	NOTE: Selecting either **Copy** or **Show Password** constitute a password "checkout". NOTE: If the password changes while you have it checked out, and your current request is still valid, select either **Copy** or **Show Password** again to obtain the new password. • Select **Hide Password** to conceal the password from view.
Approved	Select **Cancel** to remove the request. NOTE: A password release request changes from "Approved" to "Available" when the requested time is reached. It stays available until you either cancel the request or it reaches the end of the duration period.
Pending	Select **Cancel** to remove the request.
Revoked	Select **Resubmit Request** to request the password again. Select **Remove** to delete the request from the list.
Expired	Select **Remove** to delete the request from the list.
Denied	Select **Resubmit Request** to request the password again. Select **Remove** to delete the request from the list.

Approving a password release request

Depending on how the Security Policy Administrator configured the policy, a password release request will either require approval by one or more Safeguard 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 to notify you of a password release request that requires your approval. For more information, see Configuring alerts on page 25.

To approve or deny a password release request

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

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

2. Open the list of approvals and select one of 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 to **Approve** or **Deny** a password release request. Optionally, enter a comment of up to 255 characters.
Pending Additional Approvers	Select to **Deny** a password release request. Optionally, enter a comment of up to 255 characters.
Approved	Select to **Deny** or **Revoke** an approved request. 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.

NOTE: You can configure Safeguard to notify you of a password release request that requires your review. For more information, see Configuring alerts on page 25.

To review a completed password release request

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

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

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

     Optionally, enter a comment of up to 255 characters.

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

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

Session request workflow

One Identity Safeguard for Privileged Sessions allow authorized users to 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 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 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 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 Sessions can proxy and record Unix/Linux, Windows, network devices, firewalls, routers and more.

Important notes

- The Safeguard Desktop Player, used to play back recorded sessions, is installed with the Windows desktop client. However, the player is supported only on 64-bit operating systems.
- Safeguard 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**).

  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 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.

NOTE: You can configure One Identity Safeguard 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 25.

To request session access

1. From your **Home** page, click (or tap) **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.

   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 (or tap) 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 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 account(s) 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 launches an additional dialog allowing you to select the access type. Select one of the following for a session request: **RDP** or **SSH**.

     NOTE: 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 (or tap) the **— Delete** action bar 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 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 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 (or tap) the **Add to Favorites** button.

   The Add to Favorites dialog appears 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 launches 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 (or tap) **Submit Request**.

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

Taking action on a session request

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

To take action on a session request

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

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

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

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

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

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

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

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

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

State	Actions
	available until you either cancel the request or it reaches the end of the duration period.
Pending	Select **Cancel** to remove the request.
Revoked	Select **Resubmit Request** to request the session again. Select **Remove** to delete the request from the list.
Expired	Select **Remove** to delete the request from the list.
Denied	Select **Resubmit Request** to request the session again. Select **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 users, or be auto-approved.

NOTE: You can configure Safeguard to notify you of an access request that requires your approval. For more information, see Configuring alerts on page 25.

To approve or deny a sessions request

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

   NOTE: You enable or disable the **Home** page widgets in the Settings menu.
2. Open the list of approvals and select one of these view filters:

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

   NOTE: The number indicates how many requests are in that state.
3. Once you open the list, select the requester's name to see the details of the

sessions request.

4. Take the following actions on sessions requests:

State	Actions
Pending	Select to **Approve** or **Deny** a sessions request. Optionally, enter a comment of up to 255 characters.
Pending Additional Approvers	Select to **Deny** a sessions request. Optionally, enter a comment of up to 255 characters.
Approved	Select to **Deny** or **Revoke** an approved request. NOTE: You can revoke a request between the time the r equester views it and checks it in. Any eligible approver can deny an access request after i t has already been approved or auto-approved. Once dis allowed, the requester will no longer be able to access t he requested session, but he is given another opportunit y 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 25.

Launching the SSH client

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

To launch the SSH client to begin your session

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

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

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

   This makes the session request available to reviewers. If the **Record Sessions** option is enabled in the policy, the reviewer can play back the recording as part of the review process. In addition, if the **Enable 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. Select the ▶ **Launch** button to the right of the asset name. Clicking this button launches 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 action 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 to notify you of an access request that requires your review. For more information, see Configuring alerts on page 25.

To review a completed sessions request

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

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

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

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

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

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

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

      Optionally, enter a comment of up to 255 characters.

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

Replaying a session

You can play back a recorded session from the Request Workflow dialog, which can be accessed using the **Workflow** action 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 (or tapping) the icon displayed to the left of an access request session event on the activity audit log report in the Activity Center view.

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

To play back a session (Request Workflow dialog)

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

   NOTE: If accessing the Request Worklfow 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 (or tap) ▶ **Play** to launch the Safeguard Desktop Player.

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

   NOTE: If the session recording has been archived and removed from the local Safeguard file system, you will see a **Download** button instead of a ▶ **Play** button. Click (or tap) **Download** to download the recording and then click (or tap) ▶ **Play**.

3. Accept the certificate to continue.

   NOTE: On the Certificate error message, click (or tap) **Continue** to use the default Session Recording Signing certificate shipped with Safeguard. To use a different SSL certificate, click (or tap) **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 action bar 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 Desktop Player and navigating through a recording, see Recording navigation.

Safeguard Desktop Player

The Safeguard 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 Desktop Player, the main view appears, 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 10: Safeguard Desktop Player: Information tab

Control	Description
Session recording location	Displays the path of where the recording is currently stored.
Thumbnail	Click the thumbnail in the right corner of the screen to play back the recording. NOTE: The thumbnail is only available for RDP Drawing and SSH Session Shell channels. 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.
Validation indicators	The Safeguard Desktop Player checks the upstream and downstream traffic from the recording and validates the digital signature and timestamp. The

Control	Description
	indicators across the top of the screen show the results of this validation process, where all indicators should display a green check mark. If the Signature or Timestamp indicators are red Xs, this indicates that the corresponding certificate has not been validated. Contact your Appliance Administrator.
Recording details	Displays details about the recording, such as: • 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	The Channels pane displays the different types of data streams available for a recorded session. An SSH session recording will contain a single channel. Valid channels for an SSH session recording are: • **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. 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. 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
	NOTE: This channel is only available when **Allow X11 Following** is selected on the Sessions Settings tab in an access request policy. An RDP session may contain multiple channels. Valid channels for an RDP session recording are: • **Clipboard**: Contains any data that was transferred through the clipboard; there is no recording file available for play back. NOTE: This channel is only available when **Allow Clipboard** is selected on the Session Settings tab in an access request policy. • **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. Click (or tap) the ▶ **Play** button next to the channel to play back the session recording. Clicking the expansion button next to a channel displays a list of key details.

Warning tab

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

Action bar

Use the action bar buttons located at the top of the main view as described below:

Table 11: Safeguard Desktop Player action bar

Option	Description
← **Back**	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. 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 appears.
▶ **Play Channel**	Plays back the selected sessions recording.

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

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 12: Navigation controls: Playback mode

Control	Action
Timeline	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. For more information on showing or hiding the user event indicators on the timeline, see Configure seeker indicators below.
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 **Pause**	Play allows you to play the recording. 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	Allows you to display subtitles for the video that list user events as they occurred within the recorded session. User events that may appear as subtitles include windows titles, executed commands, mouse activity, and keystrokes.
Configure seeker indicators	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. NOTE: The type of user events that can be included in the timeline depends on the type of session: • RDP: Windows titles, keystrokes, mouse activity, and on-screen changes • SSH: Commands, keystrokes, and on-screen changes
Scaled video	Allows you to view the recording in a smaller or larger window. Clear this check box to play the video using the original resolution. 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.

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 13: 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 14: 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** action bar 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. On the Safeguard Desktop Player, click (or tap) **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 (or tap) 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 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 15: 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 session 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.

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
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Index

P

R

S

T

U

W