One Identity Safeguard for Privileged Sessions 5.7

Safeguard Desktop Player 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.

SPS Safeguard Desktop Player User Guide
Updated - July 2018
Version - 5.7

Contents

Summary of changes

Version 1.3 - 1.4

Changes in product:

- It is now possible to export:
  - transferred files from SCP, SFTP, and HTTP audit trails using the GUI
  - raw network traffic in PCAP format
  - screen context text from text-based protocols in TXT format

Version 1.2 - 1.3

Changes in product:

- It is now possible to jump to interesting events within an audit trail using configurable, color-coded indicators on the seeker.

  You can also choose to display subtitles for audit trails. Subtitles list certain user events as they occurred in a session.

  For details, see Replay audit trails.

Version 1.1 - 1.2

Changes in product:

- It is now possible to replay the audit trails of X11 sessions. For more information, see Replay X11 sessions.

Version 1.0 - 1.1

Changes in product:

- It is now possible to follow active connections in semi-real time. For more information, see Replay audit files in follow mode.

4

Features and limitations

CAUTION:

You can replay audit trails in your browser, or using the Safeguard Desktop Player application. Note that there are differences between these solutions.

	Browser	Safeguard Desktop Player
Works without installation	✔	-
Works on any operating system	✔	Windows, Linux
Can replay audit trails recorded with Safeguard for Privileged Sessions 5 F4 and newer	✔	✔
Can replay TN5250 sessions	✔	✔
Can extract files from SCP, SFTP, and HTTP sessions	-	✔
Can replay HTTP sessions	-	Only exports raw files from the command line
Can replay X11 sessions	✔	✔
Can start replay while rendering is in progress	-	✔
Can follow 4-eyes connections	-	✔
Can replay live streams in follow mode	-	✔
Can export to PCAP	-	✔
Can search in the trail content	✔	-
Can display user input	✔	✔
Can display subtitles for video	-	✔
Export audit trail as video	-	✔
Export screen content text	-	✔

To replay audit trails in your browser in Search (classic), see "Replaying audit trails in your browser in Search (classic)" in the Administration Guide.

For details on the Safeguard Desktop Player application, see Safeguard Desktop Player User Guide.

CAUTION:

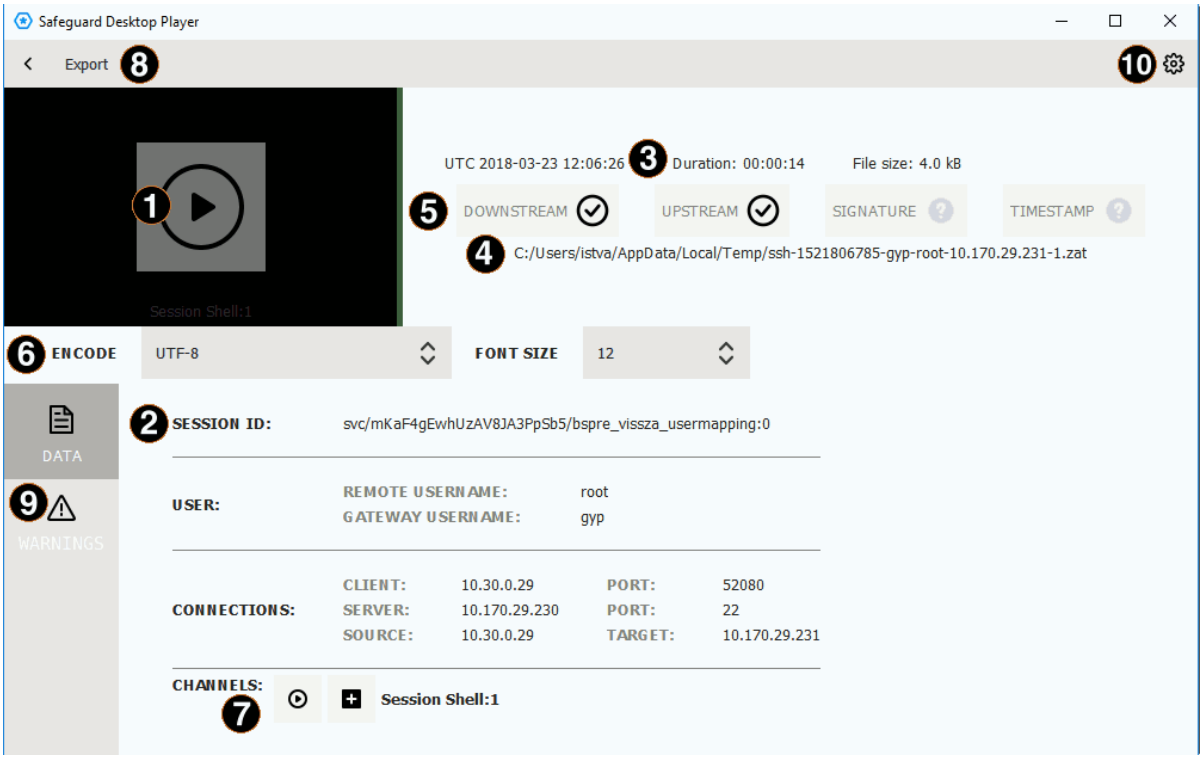
Starting with Safeguard for Privileged Sessions 5 F4, the way audit trails are encrypted has changed to make the encryption process more secure. Audit trails are now encrypted with AES-128-GCM and hashed with the SHA-512 method. This also means that in order to index and replay audit trails, you need to upgrade both your external indexers and your Safeguard Desktop Player. Earlier versions (and Audit Player) will not be able to handle audit trails (with or without encryption) recorded with Safeguard for Privileged Sessions 5 F4 and later.

First steps

Thank you for installing the Safeguard Desktop Player

Now you can start using the Safeguard Desktop Player application to replay audit trail files that you have downloaded from One Identity Safeguard for Privileged Sessions (Safeguard for Privileged Sessions). The following information will help you get started using the Safeguard Desktop Player. Note that currently this is not a public release, only a technology preview.

Getting started with the Safeguard Desktop Player



1. **Play the audit trail**

   Click the thumbnail at the top, on the left, or click ⊙ in the **Channels** section of the screen. To play an encrypted audit trail, you need to have the appropriate certificates. For details, see "Replay encrypted audit trails from the command line" in the Safeguard Desktop Player User Guide.

2. **Audit trail data**

   The most important data about the audit trail, including usernames (if available) and IP addresses. To display more metadata about a specific channel in the audit trail, click ✚ in the list of channels. These details include the parameters available on the Safeguard for Privileged Sessions **Search** page (for details, see "Searching audit trails: the Safeguard for Privileged Sessions connection database" in the Administration Guide), and other parameters, for example, the size of the desktop or the terminal.

3. **Date of the recording**

   Starting date and duration.

4. **Location of the audit trail file**

   Click the path to open the folder in your file manager.

5. **Validation results**

   When you open an audit trail, the Safeguard Desktop Player checks if you can access both the upstream and downstream traffic from the audit trail (you must have access at least to the downstream traffic to replay the audit trail), and validates the digital signature and the timestamp. The icon means that the trail is not signed or timestamped. For details, see "Validate audit trails" in the Safeguard Desktop Player User Guide.

6. **Terminal encoding and font size**

   When you are replaying terminal-based audit trails (for example, SSH or TELNET), you can set the character encoding and the font size of the displayed text. After changing the encoding or the font size, click **Re-render trail**.

7. **Replay only this channel**

   Click .

8. **Export the audit trail into a video file**

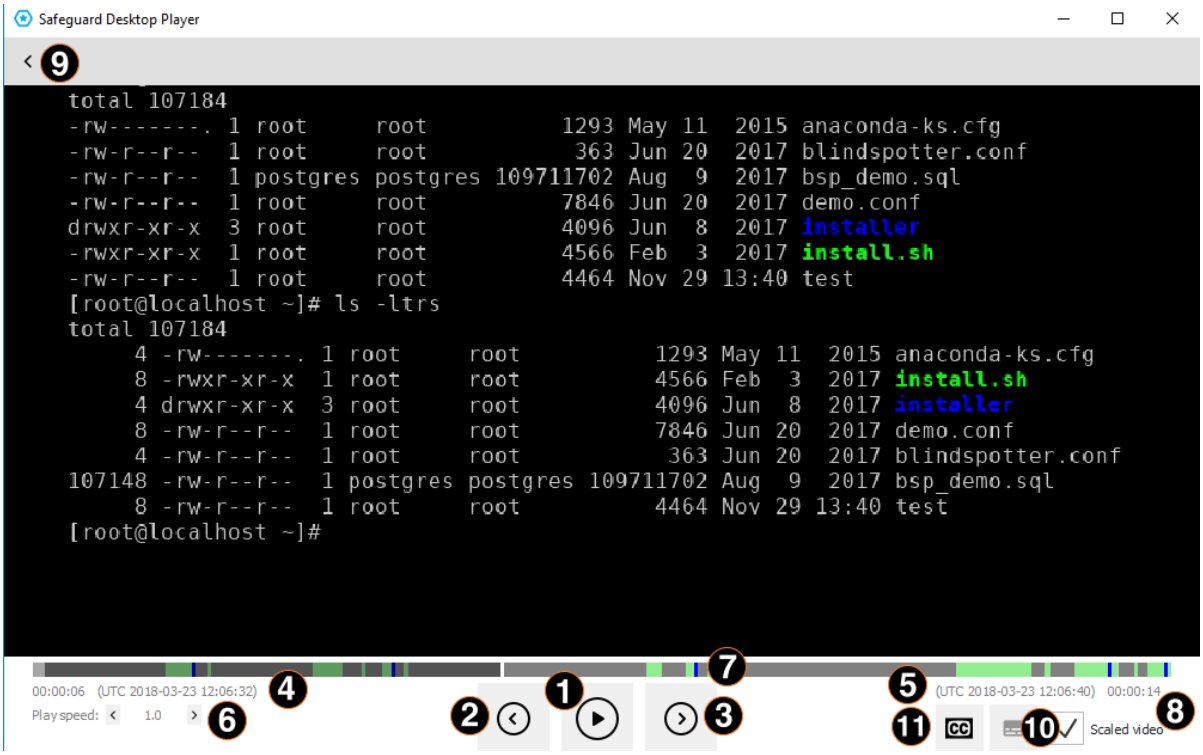
   The exported files use the WEBM format with the VP8 codec. For details, see "Export the audit trail as video" in the Safeguard Desktop Player User Guide.

9. **Warnings and errors**

   Warnings and errors that occurred during opening and processing the audit trail file.

10. **Help**

    Open the documentation in your browser.



1. **Play/pause replay**

   Start or stop replaying the audit trail. You can also click the video to start or stop replaying.

2. **Jump to previous event**

   User events that occurred in the session (such as window titles that appeared on the screen, commands executed, mouse activity, keystrokes) are marked in the seeker. Click this button to jump to the previous event.

3. **Jump to next event**

   User events that occurred in the session (such as window titles that appeared on the screen, commands executed, mouse activity, keystrokes) are marked in the seeker. Click this button to jump to the next event.

4. **Current time and timestamp**

   Time elapsed since the beginning of the audit trail, and the corresponding date.

5. **End time and timestamp**

   Length of the audit trail and the date when the session ended.

6. **Change replay speed**

7. **Seek preview**

   Click the seeker to jump to a specific location in the audit trail.

8. **Scale video**

   When enabled, the replayed audit trail is resized to fit the window. Clear to show the original size. You can also double-click on the video to toggle resizing.

9. **Back to the summary page**

   Open the summary page of the audit trail 

10. **Configure seeker indicators**

    Click to configure the visibility of indicators for user events on the seeker. Seeker indicators show on a single timeline the user events that occurred during a session. Clicking a seeker indicator takes you to the relevant user event in the audit trail. User events are window titles that appeared on the screen, commands executed, mouse activity, keystrokes, and any on-screen change.

11. **Display subtitles**

    Click to display subtitles for the video. Subtitles list user events as they occurred in the session. Events that are shown in subtitles are window titles that appeared on the screen, commands executed, mouse activity, and keystrokes.

Validate audit trails

When you open an audit trail, the Safeguard Desktop Player application automatically validates it. You can see the results of this validation above the session details.

- ⊘ is displayed if the audit trail is valid.
- ☒ is displayed if the timestamp or the signature is invalid, or the Safeguard Desktop Player could not decrypt the downstream traffic.
- **DOWNSTREAM**
  - ⊘: The downstream traffic is available and can be replayed.
  - ☒: The downstream traffic is encrypted and you do not have the decryption key. Click **Warnings** to see the fingerprint of the required certificate, and see to import it.
- **UPSTREAM**
  - ⊘: The upstream traffic is available and can be replayed.
  - ☒: The upstream traffic is encrypted and you do not have the decryption key. Click **Warnings** to see the fingerprint of the required certificate, and see to import it.
- **SIGNATURE**
  - ⊘: The trail is signed and the signature is valid.
  - ☒: The Safeguard Desktop Player could not validate the signature. Click **Warnings** to see the fingerprint of the required certificate, and see to import it.
  - ?: The audit trail is not signed.
- **TIMESTAMP**
  - ⊘: The trail is timestamped and the timestamp is valid.
  - ☒: The Safeguard Desktop Player could not validate the timestamp. Click **Warnings** to see the fingerprint of the required certificate, and see to import it.
  - ?: The audit trail is not timestamped.

Replay audit trails

Purpose:

CAUTION:

Starting with Safeguard for Privileged Sessions 5 F4, the way audit trails are encrypted has changed to make the encryption process more secure. Audit trails are now encrypted with AES-128-GCM and hashed with the SHA-512 method. This also means that in order to index and replay audit trails, you need to upgrade both your external indexers and your Safeguard Desktop Player. Earlier versions (and Audit Player) will not be able to handle audit trails (with or without encryption) recorded with Safeguard for Privileged Sessions 5 F4 and later.

To replay an unencrypted audit trail, complete the following steps.

To replay an encrypted audit trail, see .

Prerequisites:

The audit trail must be available on the computer running the Safeguard Desktop Player, or you must access it on the Shell Control Box search interface from a browser on the computer running the Safeguard Desktop Player. You can use the Safeguard for Privileged Sessions Search page to download an audit trail.

Steps:

1. Open an audit trail to replay. Use one of the following methods:
   - Start the Safeguard Desktop Player application from the menu or the command line, then click **OPEN**. Select the audit trail you want to replay.
   - Navigate to the audit trail file in a file explorer (for example, Windows Explorer), and double-click on it.
2. The Safeguard Desktop Player application displays the details of the sessions stored in the audit trail file. It automatically starts to prepare (render) the audit trail for replay. You can start replaying the audit trail while rendering is in progress, this is especially useful for long audit trails.

To start playing the audit trail, click the thumbnail at the top, on the left. If the audit trail contains more than one channels that can be replayed, select the channel to replay. Alternatively, click the icon next to the channel you want to replay.

3. The replay window opens.

   You can use the following hotkeys to control the replay:

   - Play/Pause:`SPACE`
   - Jump to previous event:`p`
   - Jump to next event:`n`
   - Enable video scaling (**Scale video**):`Ctrl+Z`
   - Toggle fullscreen replay:`f`
   - Decrease replay speed:`[`
   - Increase replay speed:`]`
   - Reset replay speed:`=`
   - Jump backward, short, medium, long:`Shift + Left Arrow`,`Alt + Left Arrow`,`Ctrl + Left Arrow`
   - Jump forward, short, medium, long:`Shift + Right Arrow`,`Alt + Right Arrow`,`Ctrl + Right Arrow`

4. To configure the visibility of seeker indicators for events, click . The **Configure seeker indicators** panel pops up:

   Use the sliders to toggle between displaying and not displaying seeker indicators for a particular event type. By default, all indicators are on.

   > TIP:
   >
   > Indicator colors represent the importance of events. The darker the color, the more important the event is. In decreasing order of importance, the colors are: dark blue > light blue > white. Classifying events this way is required so that when events overlap, there is a clear guideline as to which one of the overlapping events is shown on the seeker. It is always the more important event that will have its indicator displayed.
   >
   > In the case of the white indicators, which stand for on-screen changes, the degree of transparency signifies the volume of the change that occurred as compared to the previous on-screen change. Small changes are partly transparent white, while bigger ones are fully opaque white.

	Event type	**Shown on panel**	**Indicator color**
Application events	*Commands* Commands executed in	For terminal-	Dark blue

	Event type	Shown on panel	Indicator color
	the session-shell channel of SSH connections, or in Telnet connections.	based protocols	
Window titles Text appearing as window titles in the case of RDP, Citrix ICA, VNC, and X11 connections. This option is only displayed in the case of graphical protocols.	For graphical protocols		
User interaction	*Keystroke* Keystrokes in the session-shell channel of SSH connections, or in Telnet connections.	For all protocols	Light blue
Mouse activity Any mouse activity (clicking, scrolling, or mouse movement) in the case of RDP, Citrix ICA, and VNC connections.	For all protocols		
Other	*On-screen changes* Any change that occurred on the screen.	For all protocols	White

You can jump to interesting events by:

- Clicking any of the colored bars on the seeker.
- Clicking the ⊙ and ⊙ buttons.

5. To display subtitles for the audit trail, click CC. By default, subtitles are not displayed.

   Subtitles indicate application events (commands and window titles) and user interaction events (keystrokes and mouse activity) in the form of captions, using the colors of the event indicators.

   Subtitles are generated for all audit trails.

   When exporting audit trails as video files, you can choose to include the subtitles as well. For details, see .

Replay encrypted audit trails from the command line

Purpose:

CAUTION:

Starting with Safeguard for Privileged Sessions 5 F4, the way audit trails are encrypted has changed to make the encryption process more secure. Audit trails are now encrypted with AES-128-GCM and hashed with the SHA-512 method. This also means that in order to index and replay audit trails, you need to upgrade both your external indexers and your Safeguard Desktop Player. Earlier versions (and Audit Player) will not be able to handle audit trails (with or without encryption) recorded with Safeguard for Privileged Sessions 5 F4 and later.

To replay an encrypted audit trail using the command line, complete the following steps. Use this method if you want to import the private key only temporarily, or if you want to automate the process. To import the required certificates using the graphical interface of Safeguard Desktop Player, see .

Prerequisites:

- To replay encrypted audit trails, the private key of the certificate used to encrypt the audit trail must be available on the host running the Safeguard Desktop Player. On Microsoft Windows, the Safeguard Desktop Player can retrieve this certificate from **Windows Certificate Store > Current User > Personal Certificate Store**.
- To validate digitally-signed audit trails, the respective CA certificates that issued the certificates used to sign the audit trail must be available on the host running the Safeguard Desktop Player. (This is the CA of the certificates set at **Policies > Audit policies > Enable signing** on the Safeguard for Privileged Sessions interface.) On Microsoft Windows, the Safeguard Desktop Player can retrieve this certificate from **Windows Certificate Store > Local Computer > Trusted Root Certification Authorities**.
- To validate timestamped audit trails, the CA certificate of Safeguard for Privileged Sessions must be available on the host running the Safeguard Desktop Player. (This is the CA certificate of Safeguard for Privileged Sessions set at **Basic Settings >**

Management > SSL Certificates > CA X.509 Certificate.) On Microsoft Windows, the Safeguard Desktop Player can retrieve this certificate from **Windows Certificate Store > Local Computer > Trusted Root Certification Authorities**.

The certificates and the private keys must be available as a file in PEM format, other formats are not supported. Note that on Microsoft Windows, you cannot import CA certificates from a shared drive. In this case, copy the certificate to a local folder and import it from there.

NOTE:

Certificates are used as a container and delivery mechanism. For encryption and decryption, only the keys are used.

One Identity recommends using 2048-bit RSA keys (or stronger).

Steps:

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player. By default, it is `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\` on Microsoft Windows platforms, and `~/SafeguardDesktopPlayer` on Linux.

1. - If the private key is password-protected, execute the following command:

     ```
     player --key <path\to\your\private-key.pem>:<password-to-the-private-key>
     ```

     For example, if the private key file is `C:\temp\my-key.pem` and its password is `secret`, the command is **player --key C:\temp\my-key.pem:secret**

     Otherwise, use the following command:

     ```
     player --key <path\to\your\private-key.pem>
     ```

   - If the audit trail is timestamped or signed, you must have the proper certificate to validate the audit trail. Include the path to the certificate in the command line when starting the Safeguard Desktop Player:

     ```
     player --cert <path\to\the\certificate.pem> --key <path\to\your\private-key.pem>:<password-to-the-private-key>
     ```

2. Open the encrypted audit trail. The Safeguard Desktop Player will attempt to decrypt it with the private key you provided. If decryption is successful, you can replay the audit trail. Alternatively, you can specify the audit trail to open from the command line, for example:

   ```
   player --cert <path\to\the\certificate.pem> --key <path\to\your\private-key.pem>:<password-to-the-private-key> <path\to\audit-trail.zat>
   ```

Replay audit files in follow mode

Purpose:

CAUTION:

Starting with Safeguard for Privileged Sessions 5 F4, the way audit trails are encrypted has changed to make the encryption process more secure. Audit trails are now encrypted with AES-128-GCM and hashed with the SHA-512 method. This also means that in order to index and replay audit trails, you need to upgrade both your external indexers and your Safeguard Desktop Player. Earlier versions (and Audit Player) will not be able to handle audit trails (with or without encryption) recorded with Safeguard for Privileged Sessions 5 F4 and later.

To follow active connections in semi-real time, complete the following steps.

Prerequisites:

To be able to follow active connections, you must be permitted to authorize the sessions of the relevant connection policy. For details on how you can configure that, see .

Every time you open an `.srs` file in Safeguard Desktop Player for replay, you are required to authenticate yourself to Safeguard for Privileged Sessions through the user interface of Safeguard Desktop Player. To be able to access Safeguard for Privileged Sessions and follow active sessions, you must have:

- a valid username and password,
- the SSL certificate of your root Certificate Authority (CA).

On Microsoft Windows, the Safeguard Desktop Player retrieves the SSL certificate from *Windows Certificate Store > Local Computer > Trusted Root Certification Authorities*.

On Linux, import the SSL certificate to Safeguard Desktop Player by completing the following steps:

1. In Safeguard for Privileged Sessions, navigate to **Basic Settings > Management > SSL certificates**.
2. Click the certificate in the **CA X.509 certificate** field.
3. In the pop-up window that comes up, click **PEM**. This will download the the CA's

X.509 certificate in PEM format. The certificate must be available as a file in PEM format, other formats are not supported.

4. In Safeguard Desktop Player, click ⚙ at the top, on the right. Select **Key/Certificate import**.
5. Click ..., then select the certificate PEM file that you downloaded from Safeguard for Privileged Sessions.
6. Click **Load**. The Safeguard Desktop Player displays the details of the certificate.
7. Click **Import**.

Steps:

1. On the web interface of Safeguard for Privileged Sessions, go to **Active Connections**, and click FOLLOW next to the connection you wish to monitor in semi-real time.
2. In the Safeguard Desktop Player application, click **OPEN**, and select the audit trail to replay.

   Safeguard Desktop Player displays the sessions stored in the audit trail file.
3. Click the thumbnail to start replaying the audit file. Alternatively, click the ▶ icon next to the channel you want to replay.
4. The replay window has:

Red blinking light.

When the red blinking light is displayed, it indicates an ongoing, active connection. When neither the **LIVE** label and icon nor the red blinking light are displayed, it indicates that the connection has ended.

Blue progress bar.

LIVE status indicator.

Shows progress in the replay of the live session. When replay is paused (by hitting the Space key, clicking the **Pause** button or the video screen), the progress bar stops. It will only start progressing again, once replay is restarted (by hitting the Space key, clicking the **Play** button or the video screen).

The indicator shows three different states:

- When it is completely red, it indicates that the connection is active and there is some user interaction on the client.
- When the **LIVE** label is red but the icon is half red, half black, it indicates that the connection is active but there is no user interaction on the client.
- When neither the **LIVE** label and icon nor the red blinking light are displayed, it indicates that the connection has ended.

Gray progress bar.

Shows progress in the loading and conversion of the audit trail file to video. The bar keeps progressing until the session is active. When the video is paused, the gray bar progresses further than the blue bar, indicating to the user that there are some parts of the video that they have not watched yet.

File size.

Red light.

Displays the size of the .zat file loaded. In the case of an active, live connection, the size continuously increases.

When the red light is displayed, it indicates an ongoing, active connection. When both the **LIVE** label and icon, as well as the red light turn black, it indicates that the connection has ended.

Terminate.

Terminate the session you are monitoring if you notice some user action that poses a security risk.

LIVE status indicator.

The indicator shows three different states:

- When it is completely red, it indicates that the connection is active and there is some user interaction on the client.
- When the **LIVE** label is red but the icon is half red, half black, it indicates that the connection is active but there is no user interaction on the client.
- When both the **LIVE** label and icon are black, it indicates that the connection has ended.

TIP:

When you are replaying terminal-based audit trails (for example, SSH or TELNET), you can change the font size of the displayed text by holding down the`Ctrl`key and scrolling your mouse wheel.

When the session ends, a button is displayed. On clicking this button, the player reverts to "normal" replay mode, with options such as changing replay speed, or the seeker becoming available again.

Sharing an encrypted audit trail

Purpose:

To share an encrypted audit trail with a third party, you have two options:, complete the following steps. Note that you must open the audit trail in order to export it.

- Export the audit trail as a video file
- If you want the third party to be able to replay the audit trail with the Safeguard Desktop Player, complete the following steps. Currently you can do this only using the command line.

Prerequisites:

This procedure involves encrypting the audit trail with an encryption key that you can share with the third party. Encrypting audit trails requires an X.509 certificate in PEM format that uses an RSA key.

You will also need the audit trail file that you want to share, and the encryption key(s) required to replay it. You cannot use this procedure to encrypt an audit trail that is not already encrypted.

NOTE:

Certificates are used as a container and delivery mechanism. For encryption and decryption, only the keys are used.

One Identity recommends using 2048-bit RSA keys (or stronger).

Steps:

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player. By default, it is `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\` on Microsoft Windows platforms, and `~/SafeguardDesktopPlayer` on Linux.

1. Specify the audit trail to process, its decryption key, the new audit trail file, and the new encryption key.

Windows: **adp.exe --task rekey --file <path/to/audit-trail.zat> --key <keyfile.pem:passphrase> --out <path/to/audit-trail-to-share.zat> --new-cert <path/to/new-encryption-certificate.pem>**

Linux: **./adp --task rekey --file <path/to/audit-trail.zat> --key <keyfile.pem:passphrase> --out <path/to/audit-trail-to-share.zat> --new-cert <path/to/new-encryption-certificate.pem>**

If the audit trail is encrypted with multiple keys, repeat the `--key <keyfile.pem:passphrase>` option. Include the colon (:) character even if the key is not password-protected. For example:

```
./adp --task rekey --file /tmp/ssh-171128T1353-frobert-frobert-10.30.255.68.zat
--key /tmp/indexer-certificate-key.pem: --out /tmp/shared-ssh.zat --new-cert
/tmp/new-encryption-certificate.pem
```

2. Open the output file in the Safeguard Desktop Player and import the private key of the certificate you used to re-encrypt the audit trail. Verify that you can replay the audit trail. If it is working as expected, you can share the re-encrypted audit trail file and the private key with third parties, they will be able to replay the audit trail using the Safeguard for Privileged Sessions application.

11

Replay X11 sessions

The Safeguard Desktop Player application can replay audit trails that contain graphical X11 sessions (the contents of the **X11 Forward** channel of the SSH protocol). You can replay X11 sessions similarly to other audit trails, but note the following points.

- X11 sessions can contain several different X11 channels. For example, some applications open a separate channel for every window they display. The Safeguard Desktop Player application automatically merges these channels into a single channel, to make reviewing the sessions easier. Since these audit trails can contain SSH terminal channels as well, you can choose between replaying the SSH sessions and the X11 session in the **CHANNELS > X11** section of the audit trail data.
- If you need the list of X11 channels that the audit trail contains, they are listed in **CHANNELS > X11 > channel_ids** section of the audit trail data.
- The Safeguard Desktop Player stores the fonts used to display the texts in the audit trail in the `<desktop-player-installation-folder>/fonts` folder.

12

Export transferred files from SCP, SFTP, and HTTP audit trail

You can export the files that the user transferred in an SCP, SFTP, or HTTP session. You can export such files from the audit trails using the command line or the GUI of Safeguard Desktop Player.

Export transferred files from SCP, SFTP, and HTTP audit trail using the command line

Purpose:

To export the files that the user transferred in an SCP, SFTP, or HTTP session using the command line, complete the following steps.

Steps:

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player. By default, it is `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\` on Microsoft Windows platforms, and `~/SafeguardDesktopPlayer` on Linux.

1. List the channels in the audit trail, and find the one you want to extract files from. Note down the ID number of this channel as it will be required later on (it is 3 in the following example).

   Windows: **adp.exe --task channel-info --file <path/to/audit-trail.zat>**

   Linux: **./adp --task channel-info --file <path/to/audit-trail.zat>**

If the audit trail is encrypted, use the `--key <keyfile.pem:passphrase>` option. Repeat the option if the audit trail is encrypted with multiple keys. Include the colon (:) character even if the key is not password-protected. Example output:

```
Channel information : ssh-session-exec-scp:3
```

2. Export the files from the audit trail. Use the ID number of the channel from the previous step.

   Windows: **adp.exe --task channel-info --file <path\to\audit-trail.zat> --export-files <folder\to\save\files\>**

   Linux: **./adp --task channel-info --file <path/to/audit-trail.zat> --export-files <folder/to/save/files/>**

   If the audit trail is encrypted, use the `--key <keyfile.pem:passphrase>` option. Repeat the option if the audit trail is encrypted with multiple keys. Include the colon (:) character even if the key is not password-protected.

3. Check the output directory for the exported files.

Export transferred files from SCP, SFTP, and HTTP audit trail using the GUI

Purpose:

To export the files that the user transferred in an SCP, SFTP, or HTTP session using the GUI, complete the following steps.

Steps:

1. Open the audit trail in the Safeguard Desktop Player application.

   If the audit trail is encrypted, you need the appropriate decryption keys to open it. For details, see .

2. Click **EXPORT > Export transferred files**.

   A **Select folder** dialog box pops up.

3. Select the directory where you want to save the file(s). Click **Choose**.

   Once the export process has completed, a **FILES** dialog box pops up, indicating the number of files exported in brackets and listing the files that have been exported.

13

Export raw network traffic in PCAP format

You can choose to "convert" audit trails to packet capture (PCAP) format, which is a common file format for storing network traffic.

Export raw network traffic in PCAP format using the command line

Purpose:

To export raw network traffic in PCAP format using the command line, complete the following steps.

Steps:

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player. By default, it is `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\` on Microsoft Windows platforms, and `~/SafeguardDesktopPlayer` on Linux.

1. List the channels in the audit trail, and find the one(s) you want to export. Note down the ID number of the channel(s) as it will be required later on (it is 3 in the following example).

   Windows: **adp.exe --task channel-info --file <path/to/audit-trail.zat>**

   Linux: **./adp --task channel-info --file <path/to/audit-trail.zat>**

   If the audit trail is encrypted, use the `--key <keyfile.pem:passphrase>` option. Repeat the option if the audit trail is encrypted with multiple keys. Include the colon (:) character even if the key is not password-protected. Example output:

   ```
   Channel information : ssh-session-exec-scp:3
   ```

2. Export the channel(s) from the audit trail. Use the ID number(s) of the channel(s)

from the previous step.

Windows: **adp.exe -f <path/to/audit-trail.zat> -c <channel id> -t indexer --export-pcap output.pcap**

Linux: **adp -f <path/to/audit-trail.zat> -c <channel id> -t indexer --export-pcap output.pcap**

If the audit trail is encrypted, use the `--key <keyfile.pem:passphrase>` option. Repeat the option if the audit trail is encrypted with multiple keys. Include the colon (:) character even if the key is not password-protected.

3. Check the output directory for the exported files.

Export raw network traffic in PCAP format using the GUI

Purpose:

To export the channels stored in the audit trail using the GUI, complete the following steps.

Steps:

1. Open the audit trail in the Safeguard Desktop Player application.

   If the audit trail is encrypted, you need the appropriate decryption keys to open it. For details, see .

2. Click **EXPORT > Export pcap**.

   A **Select folder** dialog box pops up.

3. Select the directory where you want to save the file(s). Click **Choose**.

   Once the export process has completed, a **FILES** dialog box pops up, indicating the number of files exported in brackets and listing the files that have been exported.

   Files have a number in their names, used for identifying the channels.

Export screen content text

Purpose:

To export screen content text from text-based protocols (that is, terminal-based protocols and HTTP) in TXT format, complete the following steps. Screen content text is saved into files as UTF-8 encoded text with UNIX timestamps.

Steps:

1. Open the audit trail in the Safeguard Desktop Player application.

   If the audit trail is encrypted, you need the appropriate decryption keys to open it. For details, see .

2. Click **EXPORT > Export screen content text**.

   A **Select folder** dialog box pops up.

3. Select the directory where you want to save the file(s). Click **Choose**.

   Once the export process has completed, a **FILES** dialog box pops up, indicating the number of files exported in brackets and listing the files that have been exported.

   Filenames follow a pattern. Take the following example:

   `1415176790.648000-1415176793.926000.txt`

   Where:

   - the numbers before the hyphen (-) indicate the beginning of the interval in the session where the screen content text occurred
   - the numbers after the hyphen (-) indicate the end of the interval in the session where the screen content text occurred
   - the numbers are provided in UNIX timestamp format

15

Troubleshooting the Safeguard Desktop Player

Determine your Safeguard Desktop Player version

To find out which version of the Safeguard Desktop Player application you are using, complete one of the following.

- Start the Safeguard Desktop Player application, and on the opening screen, click ... > **About**. This displays the version number of Safeguard Desktop Player and also the underlying **adp** application.
- Execute the following commands from the command line in the directory where Safeguard Desktop Player is installed:

  Windows: **adp.exe --version & player.exe --version**

  Linux: **./adp --version; ./player --version**

.zat and .srs files are not opened automatically

On Linux, if you are not using a Desktop Manager (for example, GNOME, KDE, Unity), and you are installing the Safeguard Desktop Player with user privileges, registering the `.zat` and `.srs` files to the Safeguard Desktop Player might fail. To solve this problem, perform a system-wide installation (run the installer with **sudo**).

Problems in VirtualBox

If fonts are not displayed correctly, or the Safeguard Desktop Player application crashes when started in VirtualBox, ensure that you have 3D acceleration enabled (`Machine > Settings > Display > Screen > Enable 3D Acceleration`), and install VirtualBox Guest Additions.

If these do not solve the problem, see Troubleshooting the Safeguard Desktop Player.

Force software rendering

Some video card drivers might have issues with OpenGL rendering: fonts do not appear correctly, or the Safeguard Desktop Player application crashes when started with warnings about the graphics card. If this happens, Safeguard Desktop Player tries to fall back to software rendering, but it might fail to do so.

To force software rendering, start the Safeguard Desktop Player using the **Safeguard Desktop Player - software rendering** item in your application menu, or with the `--software` command-line option:

- *Windows*: **player.exe --software**
- *Linux*: **./player --software**

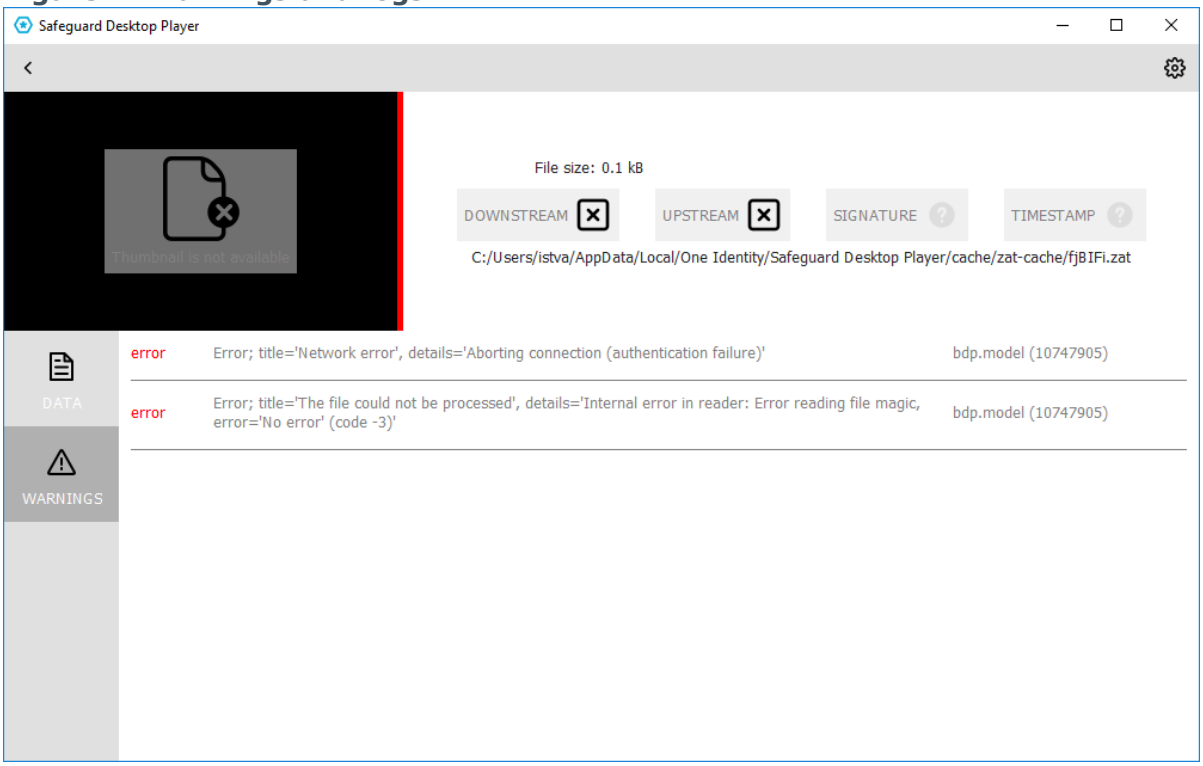
Cannot import CA certificate

Note that on Microsoft Windows, you cannot import CA certificates from a shared drive. In this case, copy the certificate to a local folder and import it from there. Also, the Safeguard Desktop Player application must be installed locally, you cannot start the `player.exe` file from a shared drive.

Logging

The Safeguard Desktop Player application displays important log messages on the **Warnings** tab. If you increase the log level of the application above the default, additional log messages are also displayed.

Figure 1: Warnings and logs



You can use the following command-line parameters to specify the log level of the Safeguard Desktop Player application.

- **-l** or **--log-level** <number>
- Set the log level of Safeguard Desktop Player. The default is 3, 0 completely disables logging, 7 is the most verbose, used for debugging. For example:

  Windows: **player.exe --log-level 5**

  Linux: **./player --log-level 5**
- **-o** or **--log-output** <path-to-logfile>
- Specify the path and filename of the log file. For example:

  Windows: **player.exe --log-output desktop-player.log**

  Linux: **./player --log-output /tmp/desktop-player.log**
- **-s** or **--log-spec** <log-spec>
- Specify different log levels for certain components of Safeguard Desktop Player. For example:

  Windows: **player.exe --log-level 3 --log-spec "bdp.core:5"**

  Linux: **./player --log-level 3 --log-spec "bdp.core:5"**

Install Safeguard Desktop Player

System requirements

The Safeguard Desktop Player application supports the following platforms:

- **Microsoft Windows:**

  64-bit version of Windows 7 or newer. Install the appropriate driver for your graphic card.

- **Linux:**

  RHEL 6, CentOS 6, or newer. The Safeguard Desktop Player application will probably run on other distributions as well that have at least libc6 version 2.12 installed.

Installing the Safeguard Desktop Player application requires about 120MB disk space, and a temporarily used disk space to store the audit trails that are replayed. The size of the temporary files depends on the size of the replayed audit trails.

You can install the Safeguard Desktop Player application with user privileges.

Install Safeguard Desktop Player on Windows

Purpose:

To install the Safeguard Desktop Player application, complete the following steps.

Prerequisites:

- You must have a valid support portal account with access to Shell Control Box downloads.

- **Microsoft Windows:**

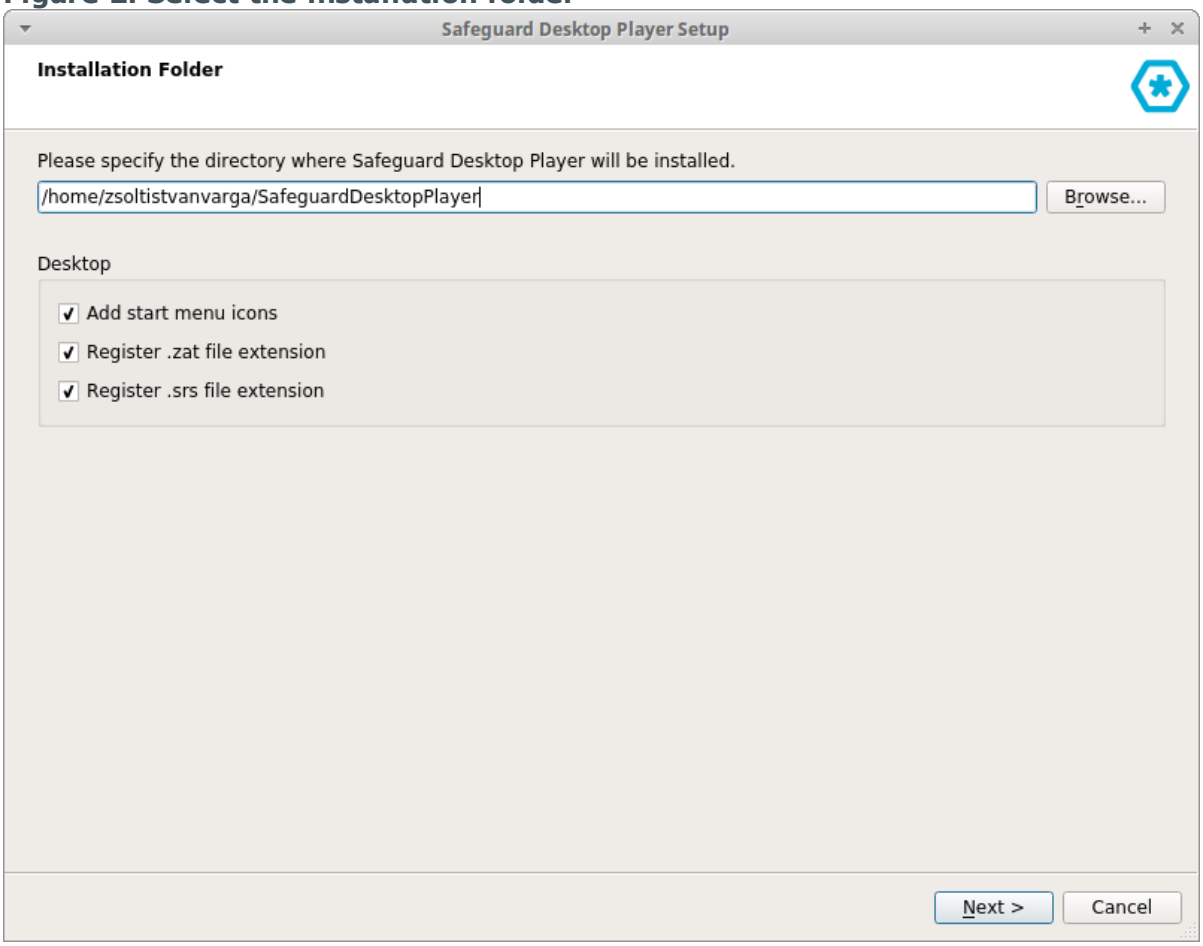
  64-bit version of Windows 7 or newer. Install the appropriate driver for your graphic card.

  For details, see Install Safeguard Desktop Player.

- If you already have an earlier version of the Safeguard Desktop Player application installed on the host, uninstall the previous installation. If you want to keep the previous installation for some reason, install the new version into a different directory.

Steps:

Figure 2: Select the installation folder



Select the installation folder for the Safeguard Desktop Player application, then click **Next**.

The default installation folder is `C:\Program Files\Safeguard Desktop Player` on Microsoft Windows, and `~/SafeguardDesktopPlayer` on Linux.

Click **Next**.

Read the end-user license agreement of Safeguard Desktop Player, select **I accept the license**, then click **Next**. You can also find the end-user license agreement at Administration Guide.

Click **Install** to install the Safeguard Desktop Player application, then **Finish** when the installation is complete.

1. Download the Safeguard Desktop Player application for Windows from the Downloads page.
2. - *Install for the current user*: Navigate to the download directory and start the downloaded file.
   - *Install for every user (system-wide installation)*: Open a command prompt, and navigate to the download directory. Then start the downloaded file with the `AllUsers=true` parameter. For example: **desktop_player_ installer.1.0.28.release.exe AllUsers=true**

   The installation wizard opens. Click **Next**.

Install Safeguard Desktop Player on Linux

Purpose:

To install the Safeguard Desktop Player application, complete the following steps.

Prerequisites:

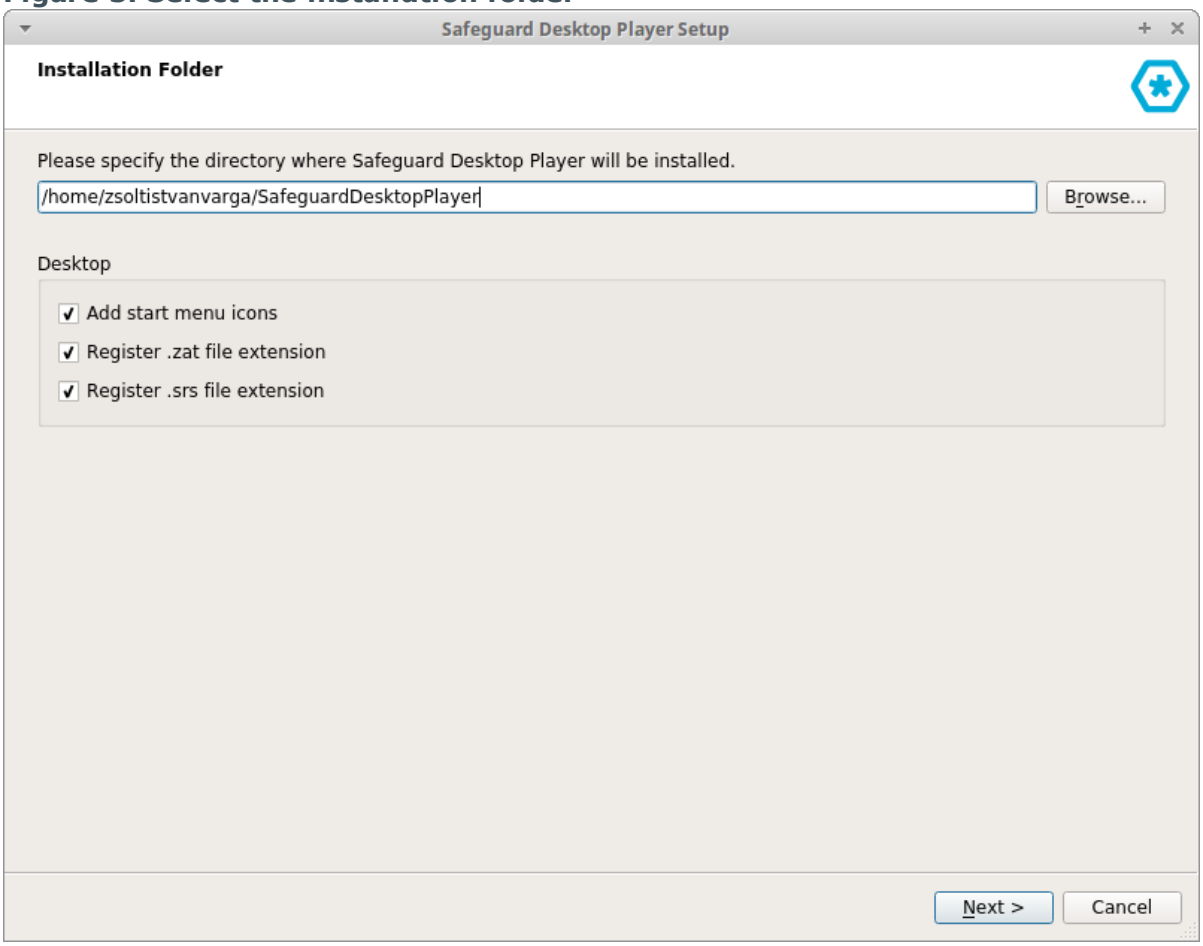
- You must have a valid support portal account with access to Shell Control Box downloads.
- **Linux:**

  RHEL 6, CentOS 6, or newer. The Safeguard Desktop Player application will probably run on other distributions as well that have at least libc6 version 2.12 installed.

  For details, see Install Safeguard Desktop Player.
- If you already have an earlier version of the Safeguard Desktop Player application installed on the host, uninstall the previous installation. If you want to keep the previous installation for some reason, install the new version into a different directory.

Steps:

Figure 3: Select the installation folder



Select the installation folder for the Safeguard Desktop Player application, then click **Next**.

The default installation folder is `C:\Program Files\Safeguard Desktop Player` on Microsoft Windows, and `~/SafeguardDesktopPlayer` on Linux.

Click **Next**.

Read the end-user license agreement of Safeguard Desktop Player, select **I accept the license**, then click **Next**. You can also find the end-user license agreement at Administration Guide.

Click **Install** to install the Safeguard Desktop Player application, then **Finish** when the installation is complete.

1. Download the Safeguard Desktop Player application for Linux from the Downloads page.
2. Open a terminal, and navigate to the download directory.
3. Start the downloaded file.

- *Install for every user (system-wide installation)*: System-wide installation requires root privileges. To install Safeguard Desktop Player for every user on the host, issue the following commands:

  ```
  chmod +x ./desktop_player_installer.1.0.17.release.run; sudo ./desktop_player_installer.1.0.17.release.run
  ```

- *Install for the current user*: You can install the Safeguard Desktop Player application with user privileges. To install Safeguard Desktop Player for the current user on the host, issue the following commands:

  ```
  chmod +x ./desktop_player_installer.1.0.17.release.run; ./desktop_player_installer.1.0.17.release.run
  ```

The installation wizard opens. Click **Next**.

17

Keyboard shortcuts

You can use the following hotkeys to control the replay.

- Play/Pause:`SPACE`
- Jump to previous event:`p`
- Jump to next event:`n`
- Enable video scaling (**Scale video**):`Ctrl+Z`
- Toggle fullscreen replay:`f`
- Decrease replay speed:`[`
- Increase replay speed:`]`
- Reset replay speed:`=`
- Jump backward, short, medium, long:`Shift + Left Arrow,Alt + Left Arrow,Ctrl + Left Arrow`
- Jump forward, short, medium, long:`Shift + Right Arrow,Alt + Right Arrow,Ctrl + Right Arrow`

About us

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

Contacting us

For sales 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