One Identity Safeguard for Privileged Sessions 7.1.1

Safeguard Desktop Player User Guide

Legend

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

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

SPSSafeguard Desktop Player User Guide
Updated - 05 January 2023, 12:27

For the most recent documents and product information, see Online product documentation.

Contents

Summary of changes

Version 1.8 - 1.9

Changes in product:

- For RDP and ICA trails, you can select a keyboard layout depending on the language used in the trail and recreate the subtitle of the trail.

  For more information, see Replaying audit trails.
- The installation of the Safeguard Desktop Player on Windows has been improved. You no longer need elevated privileges to install the Safeguard Desktop Player, and for future versions, you can install the new version without first having to uninstall the previous version.

  If you already have an earlier version of the Safeguard Desktop Player application installed on the host (version 1.8 or earlier), uninstall the previous installation. For future versions of the Safeguard Desktop Player, you do not need to uninstall the previous version before you can install the new version as this will be done automatically.

  For more information, see Installing Safeguard Desktop Player on Windows.

Version 1.6 - 1.8

Changes in product:

- It is now possible to export transferred files from the clipboard channel in RDP sessions.

  For more information, see Exporting transferred files from SCP, SFTP, HTTP, and RDP audit trails.

Version 1.5 - 1.6

Changes in product:

- It is now possible to search in the contents of the audit trails for trails of graphical sessions created and indexed with SPS 6.0.

  For more information, see Searching in the content of the current audit file.

Version 1.4 - 1.5

Changes in product:

- It is now possible to install the Safeguard Desktop Player application on Mac.

  For more information, see Installing Safeguard Desktop Player on Mac.

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 Replaying 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 Replaying 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 Replaying audit files in follow mode.

Features and limitations

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

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

The following table details the differences between the solutions provided by the browser and the Safeguard Desktop Player application when replaying audit trails.

	Browser	Safeguard Desktop Player
Works without installation	✓	-
Works on any operating system	✓	Windows, Linux, Mac
Replays audit trails recorded with SPS 5 F4 and newer	✓	✓
Replays TN5250 sessions	✓	✓
Extracts files from SCP, SFTP, HTTP and RDP sessions	-	✓
Replays HTTP sessions	-	Only exports raw files from the command line
Replays X11 sessions	✓	✓
Starts replay while rendering is in progress	✓	✓
Follows 4-eyes connections	-	✓
Replays live streams in follow mode	✓	✓
Exports to PCAP	-	✓
Displays user input	✓	✓
Displays subtitles for video	✓	✓
Exports audit trail as video	-	✓

	Browser	Safeguard Desktop Player
Exports screen content text	-	✓
Searches in the contents of the audit trails	-	✓

Installing Safeguard Desktop Player

This section provides information on how to install the Safeguard Desktop Player application in different operating systems.

Safeguard Desktop Player system requirements

The Safeguard Desktop Player application supports the following operating systems:

- **Microsoft Windows:**

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

- **Linux:**

  RHEL 7, CentOS 7, or newer. The Safeguard Desktop Player application will probably run on other distributions as well that have at least libc6 version 2.17 installed.

  Depending on the distribution, you will need to install the following packages:

  - On Debian-based GNU/Linux:
    - libxcb-render-util0
    - libxcb-keysyms1
    - libxcb-image0
    - libxcb-randr0
    - libxcb-xkb1
    - libxcb-xinerama0
    - libxcb-icccm4
  - On CentOS/Red Hat:

- xcb-util-renderutil
- xcb-util-keysyms
- xcb-util-image

- **Mac:**

  macOS Catalina 10.15, or newer.

To install the Safeguard Desktop Player application, you need about 200MB 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.

Installing Safeguard Desktop Player on Windows

This section describes how to install the Safeguard Desktop Player application.

NOTE: If you use the SPP desktop client application to view audit trails that were created and indexed with One Identity Safeguard for Privileged Sessions (SPS), see Installing Safeguard Desktop Player on Windows to use with the SPP desktop client application.

Prerequisites

- You must have a valid support portal account with access to SPS downloads.
- **Microsoft Windows:**

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

  For details, see Safeguard Desktop Player system requirements.
- If you already have an earlier version of the Safeguard Desktop Player application installed on the host (version 1.8 or earlier), uninstall the previous installation. For future versions of the Safeguard Desktop Player, you do not need to uninstall the previous version before you can install the new version as this will be done automatically.

To install the Safeguard Desktop Player application

1. Download the Safeguard Desktop Player application for Windows from the Downloads page.
2. Install the Safeguard Desktop Player application using one of the following options:

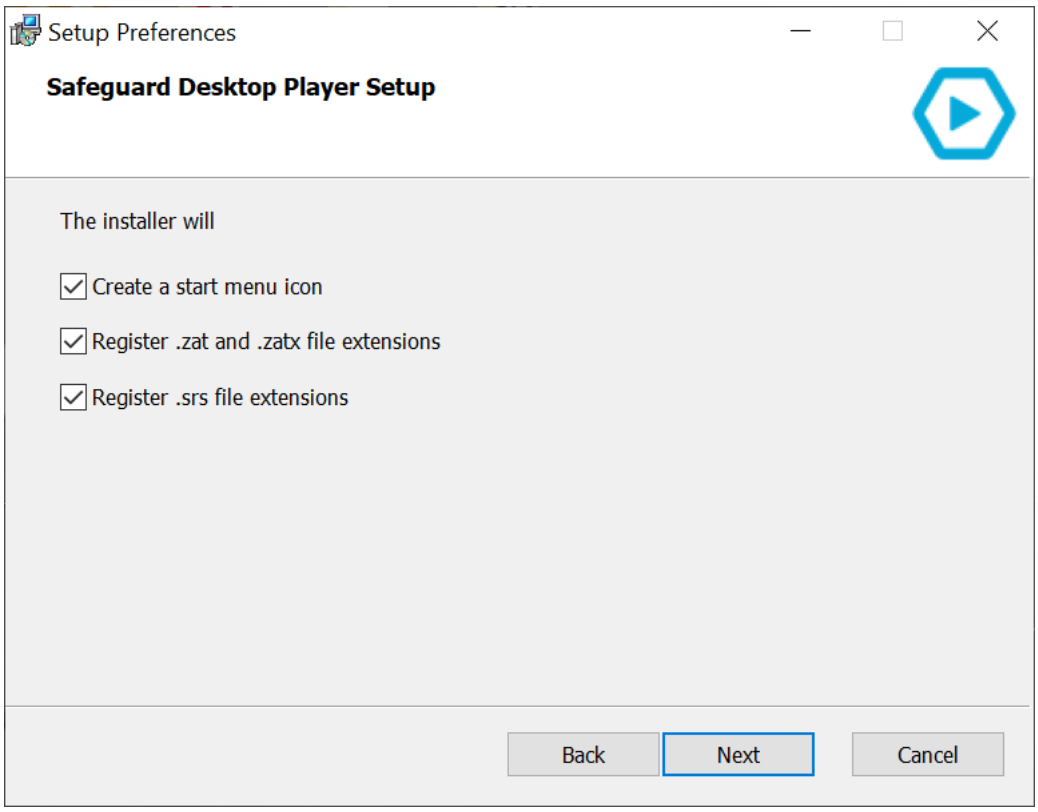
- Navigate to the `Downloads` directory and start the installation.
- *Silent install if using terminal*: Alternatively, from the terminal, use the **`msiexec /quiet`** silent install option to install the Safeguard Desktop Player.

  For example: `msiexec /i <player.msi> INSTALLFOLDER="C:\Users\<yourusername>\AppData\Local\Safeguard\" /quiet`

The installation wizard opens.

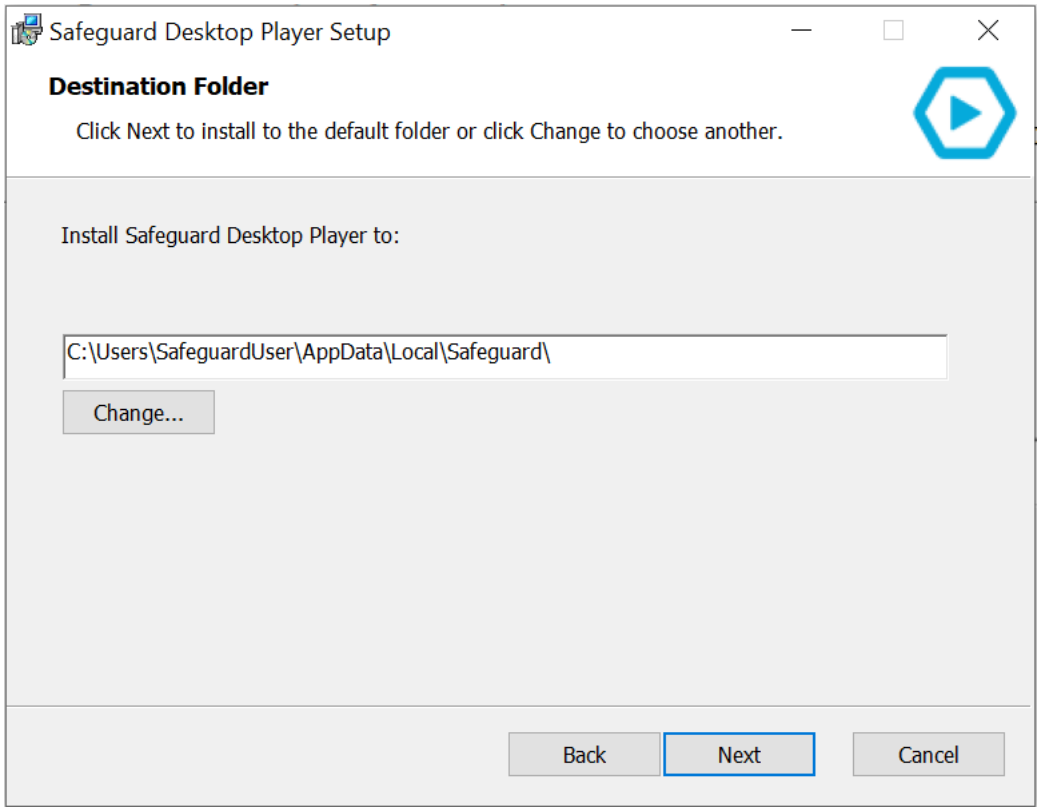
3. On the **Setup Preferences** page, select the required options. After that, click **Next** to create the start menu icon, and register the audit trail file extensions.

Figure 1: Setup preferences



4. Select where you want to save the Safeguard Desktop Player application installer, and after that, click **Next**. The default installation folder is `C:\Users\<yourusername>\AppData\Local\Safeguard`.

Figure 2: Selecting the installation folder



5. Read the Software Transaction, License and End User License Agreements of Safeguard Desktop Player, select **I accept the license**, then click **Next**.
6. To install the Safeguard Desktop Player application, click **Install**, and after that, when the installation is complete, click **Finish**.

Installing Safeguard Desktop Player on Windows to use with the SPP desktop client application

This section describes how to install the Safeguard Desktop Player application if you use the One Identity Safeguard for Privileged Passwords (SPP) desktop client application to view audit trails for trails created and indexed with One Identity Safeguard for Privileged Sessions (SPS).

From Safeguard Desktop Player version 1.9, the default installation folder on Microsoft Windows has changed from `C:\Program Files\Safeguard\Safeguard Desktop Player` to `C:\Users\<yourusername>\AppData\Local\Safeguard\`. SPP still looks for Safeguard Desktop Player at the previous location, that is, `C:\Program Files\Safeguard Desktop Player`.

When installing Safeguard Desktop Player version 1.9 or later to use with the SPP desktop client application, change the default installation folder to `C:\Program Files\Safeguard\Safeguard Desktop Player` as described below.

Prerequisites

- You must have a valid support portal account with access to SPS downloads.
- **Microsoft Windows:**

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

  For details, see Safeguard Desktop Player system requirements.
- If you already have an earlier version of the Safeguard Desktop Player application installed on the host (version 1.8 or earlier), uninstall the previous installation.

To install the Safeguard Desktop Player application on Windows to use with the SPP desktop client application

1. Download the Safeguard Desktop Player application for Windows from the Downloads page.
2. Open a terminal with elevated privileges.
3. Enter **`msiexec /i <player.msi> INSTALLFOLDER="C:\ProgramFiles\Safeguard" /quiet`**

   The Safeguard Desktop Player is installed at `C:\Program Files\Safeguard Desktop Player` and you can use it with the SPP desktop client application.

Installing Safeguard Desktop Player on Linux

This section describes how to install the Safeguard Desktop Player application.

Prerequisites

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

  RHEL 7, CentOS 7, or newer. The Safeguard Desktop Player application will probably run on other distributions as well that have at least libc6 version 2.17 installed.

  For details, see Safeguard Desktop Player system requirements.
- 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 in a different directory.

To install the Safeguard Desktop Player application

1. Download the Safeguard Desktop Player application for Linux from the Downloads page.
2. Open a terminal, and navigate to the `Downloads` directory.
3. To install the Safeguard Desktop Player application, start the downloaded file.
   - *Installing 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
     ```

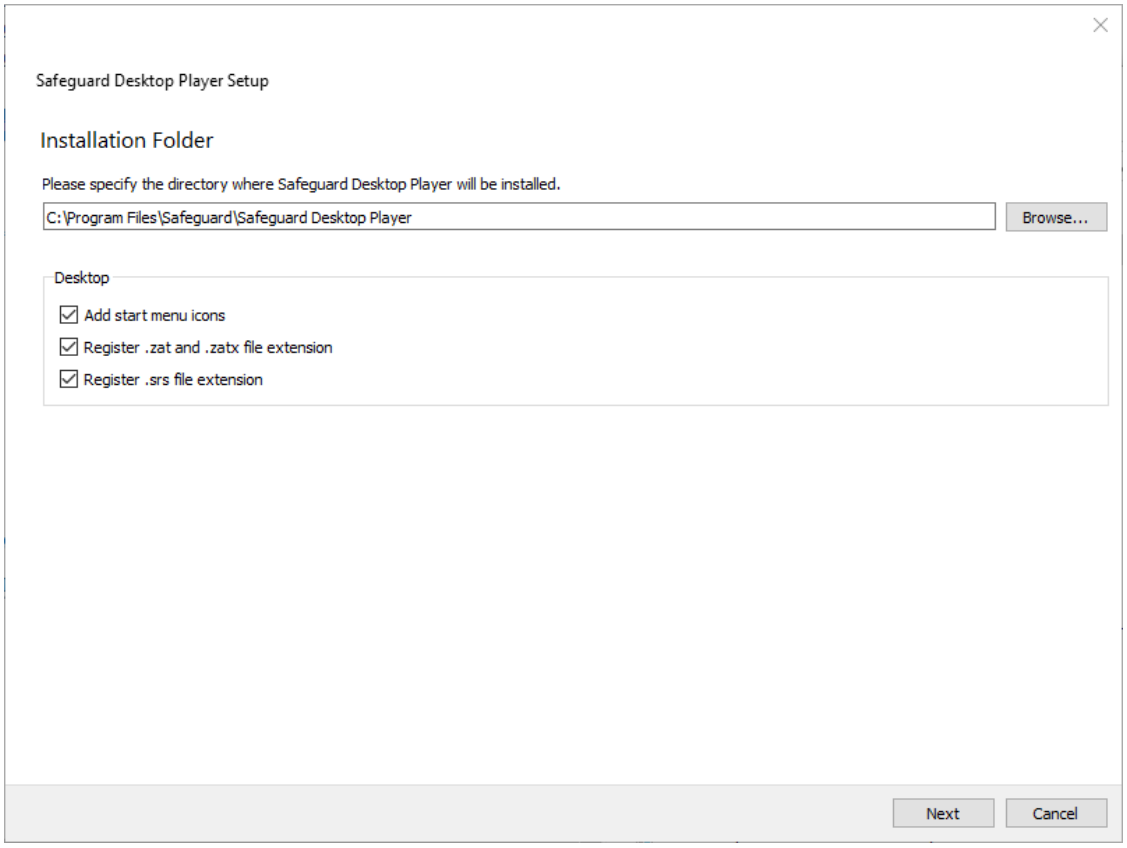
   - *Installing for the current user*: You can install the Safeguard Desktop Player application with user privileges. To install Safeguard Desktop Player for the current user on the host, issue the following commands:

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

   The installation wizard opens. Click **Next**.
4. Select the folder where you want to install the Safeguard Desktop Player application, and after that click **Next**.

   The default installation folder on Linux is `~/SafeguardDesktopPlayer`.

Figure 3: Selecting the installation folder



5. Read the Software Transaction, License and End User License Agreements of Safeguard Desktop Player, select **I accept the license**, then click **Next**.
6. To install the Safeguard Desktop Player application, click **Install**, then click **Finish** when the installation is complete.

Installing Safeguard Desktop Player on Mac

This section describes how to install the Safeguard Desktop Player application.

Prerequisites

- You must have a valid support portal account with access to SPS downloads.
- MacOS High Sierra 10.13, or newer.

  For details, see Safeguard Desktop Player system requirements.

- 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 in a different directory.

To install the Safeguard Desktop Player application

1. Download the Safeguard Desktop Player application for Mac from the Downloads page.
2. Double-click the **desktop_player_installer.version.release.dmg** to open the installer, then drag the Safeguard Desktop Player application to the `Applications` folder.

Figure 4: Drag the application to the `Applications` folder

3. If your Mac is set to allow applications only from the App Store, you get a warning that you cannot install the application. You can temporarily override your Mac security settings and open the application as follows:

Figure 5: Safely open apps on your Mac — Warning message

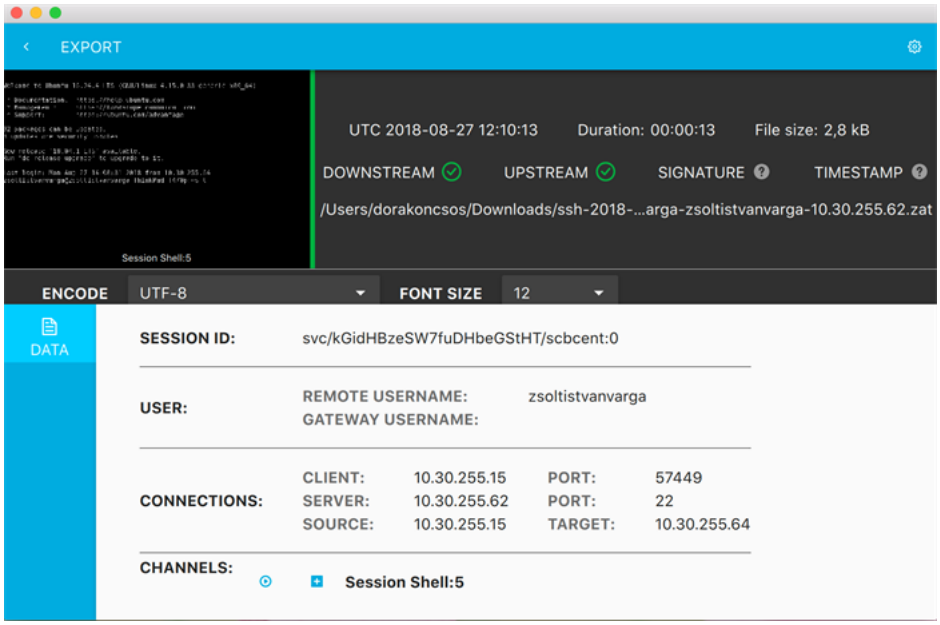
a. In **Finder**, press `Control` and click the Safeguard Desktop Player application.

b. Select **Open** from the menu, and in the dialog that appears, click **Open**.

   The Safeguard Desktop Player application is now saved as an exception to your security settings, and you can open it by double-clicking it.

4. Open an audit trail that you want to replay. For more information, see Replaying audit trails.

Figure 6: Replaying an audit trail



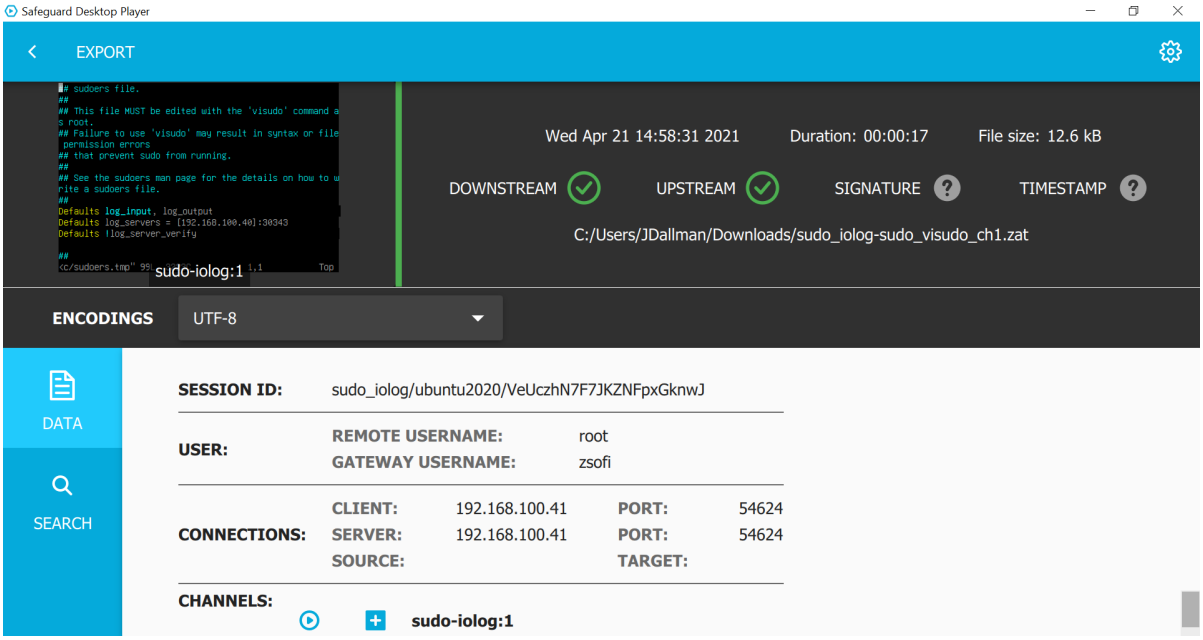
First steps

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 (SPS). This guide will help you to get started with using the Safeguard Desktop Player.

The following figure displays the UI of the Safeguard Desktop Player application.

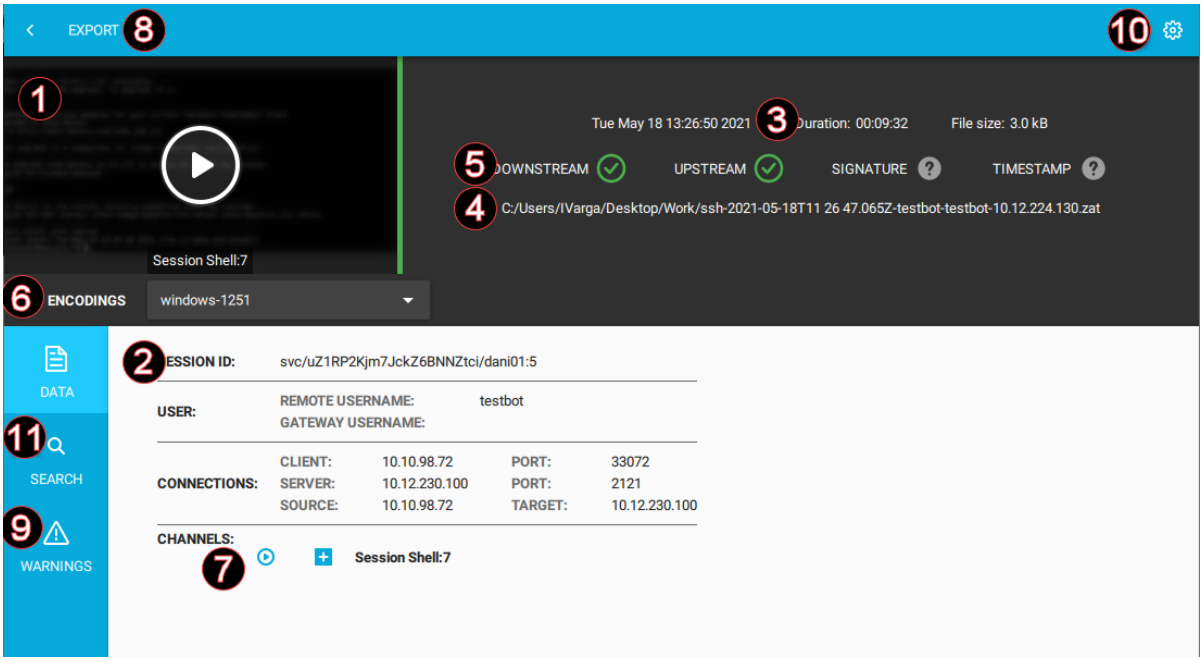
Figure 7: Safeguard Desktop Player



Getting started with the Safeguard Desktop Player

This section shortly describes the main functions and the UI elements of the Safeguard Desktop Player.

Figure 8: Safeguard Desktop Player > Details page



1. Audit trail play button

   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 "Replaying encrypted audit trails" 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 SPS **Search** page (for details, see "Using the Search interface" 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 "Validating audit trails" in the Safeguard Desktop Player User Guide.

6. Terminal **Encodings**

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

7. **Channels**

   To select a channel, click .

8. **Export**

   The **Export** button exports the audit trail to a video file. The exported files use the WEBM format with the VP8 codec. For details, see "Exporting the audit trail as video" in the Safeguard Desktop Player User Guide.

9. **Warnings**

   Warnings and errors that occurred during opening and processing the audit trail file. If there are warnings or errors, the **Warnings** UI element is displayed under the **Search** field.

   Figure 9: Warnings

10. Settings

    You have the following settings options:

    - Import the required certificate to replay an encrypted audit trail. For more information, see Replaying encrypted audit trails.
    - Open **Preferences**, which you can use to set the application language, select a keyboard layout, select how you want to display the window title events on the seeker and in subtitles, and so on. For more information, see Preferences for the Safeguard Desktop Player.
    - Open the documentation in your browser.

11. **Search**

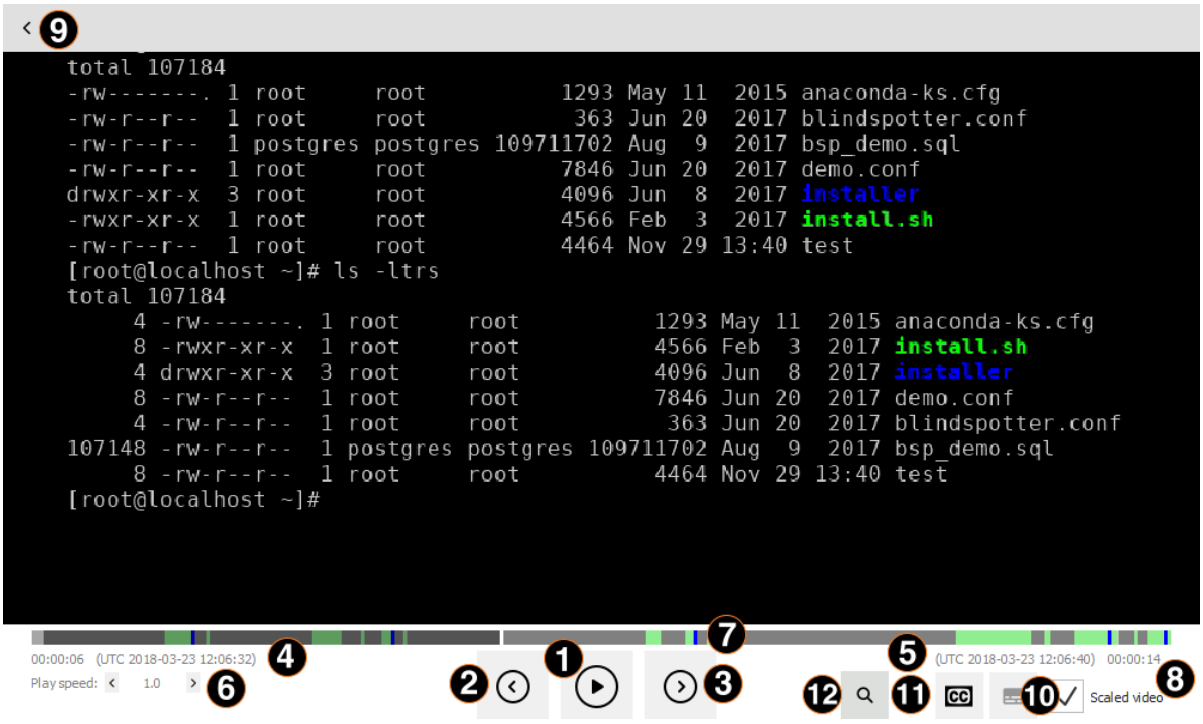
You can search in the trail content of the current audit trail, for example, in commands that the user executed in the session, or to find a specific text that was displayed on the screen. Available only for terminal sessions. For details, see Searching in the content of the current audit file.

The Search window of Safeguard Desktop Player

This section provides information on the options that you can use in the **Search** window.

Search

You can search in the trail content of the current audit trail, for example, in commands that the user executed in the session, or to find a specific text that was displayed on the screen. Available only for terminal sessions. For details, see Searching in the content of the current audit file.



1. Play/pause, replay

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

2. Jump to previous event

Click this button to jump to the previous user 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.

3. Jump to next event

   Click this button to jump to the 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.

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.

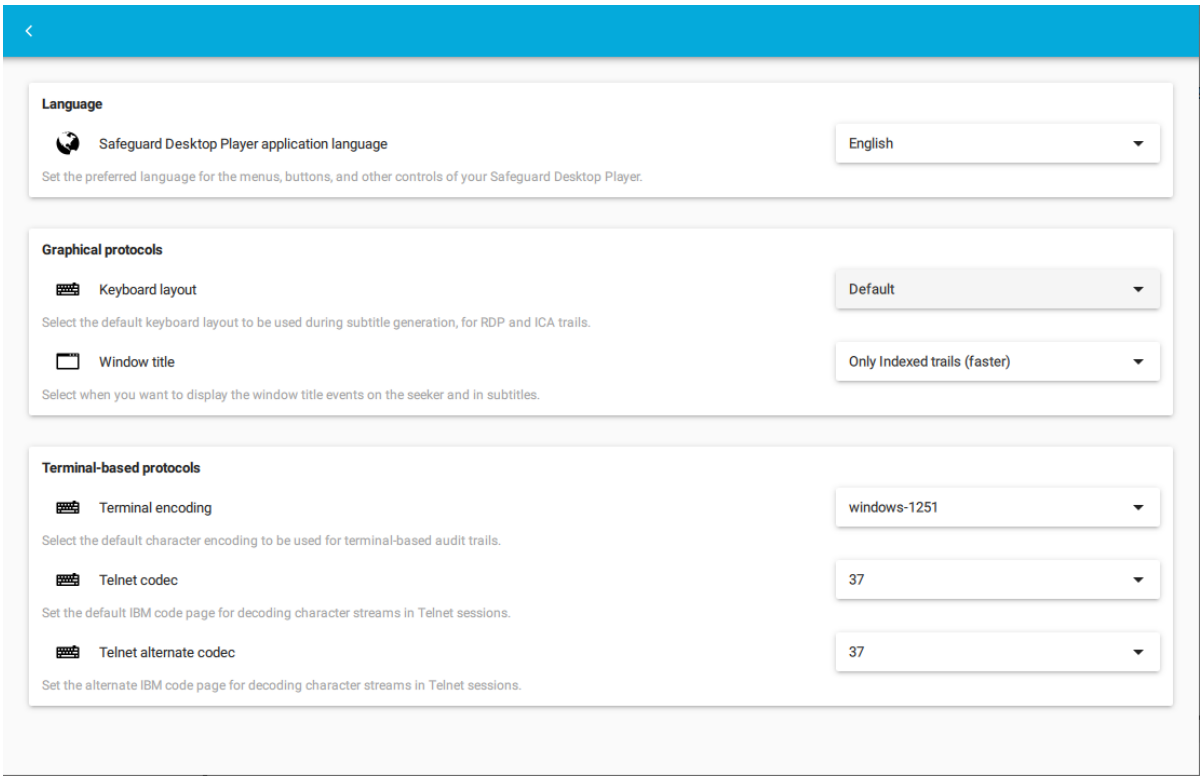
12. Search in trail content

    Search in the contents of the current audit trail, for example, in commands that the user executed in the session, or to find a specific text that was displayed on the screen. This option is available only for terminal sessions. For details, see Searching in the content of the current audit file.

Preferences for the Safeguard Desktop Player

To configure your global preferences, for example, the application language, keyboard layout, and so on, for Safeguard Desktop Player, navigate to **(Settings)** > **Preferences**.

Figure 10: Settings > Preferences



Language

- **Safeguard Desktop Player application language**: Set the preferred language for the menus, buttons, and other controls of your Safeguard Desktop Player.

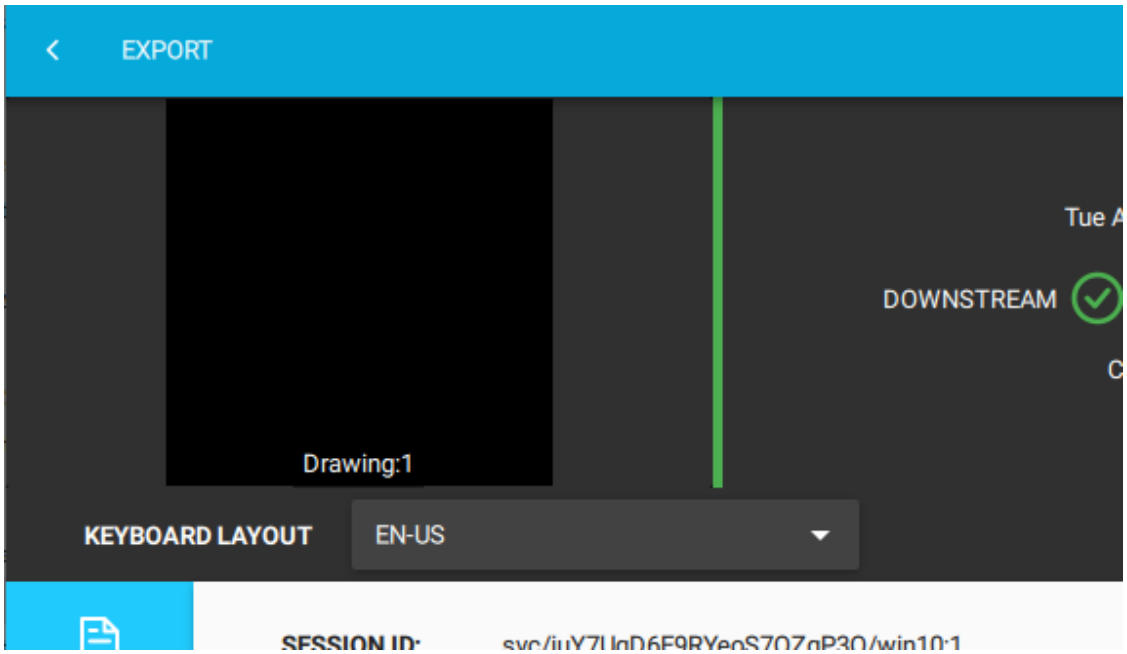
  For the changes to take effect, close and restart the Safeguard Desktop Player application.

Graphical protocols

- **Keyboard layout**: In some cases, RDP and ICA audit trails do not contain their specific keyboard layouts. To avoid misspellings in the subtitles, you can set your specific layout for all your audit trails.

  For each individual audit trail, you can still override these global settings from your **Details** page of your Safeguard Desktop Player as shown in the example figure below:

  Figure 11: Safeguard Desktop Player > Details page > Changing the keyboard layout for individual RDP or ICA audit trails

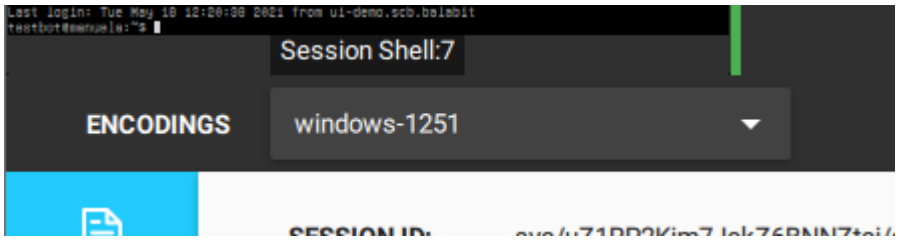
- **Window title**: Select how you want to display the window title events on the seeker and in subtitles.
  - If your audit trails are indexed, select **Only indexed trails (faster)**. Indexed audit trails already contain the window titles, and the process of displaying the window titles is faster.
  - If you are unsure whether your audit trails are indexed, select **Always**. Safeguard Desktop Player detects if your audit trails are indexed. If no indexed audit trail is available, Safeguard Desktop Player will start indexing the audit trails automatically.
  - If your audit trails are not indexed, select **Forced detection (slower)**. The audit trail will be re-indexed, regardless if it had been indexed before or not, and as a result, the process of displaying the window titles is slower.
  - If you do not want to display window titles, select **Never**.

Terminal-based protocols

- **Terminal encoding**: The character encoding of the displayed text on terminal-based audit trails, for example, SSH, Telnet or Sudo iolog. This selection will be your default encoding.

  For each individual audit trail, you can still override these global settings from your **Details** page of your Safeguard Desktop Player as shown in the example figure below:

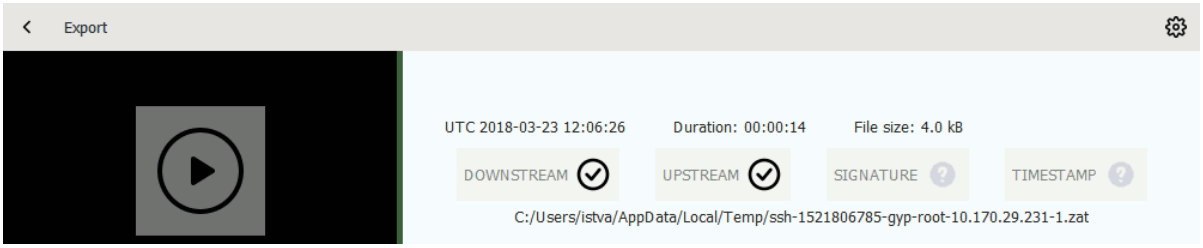
  Figure 12: Safeguard Desktop Player > Details page > Changing the encoding for individual audit trails

- **Telnet codec**: To deal with special characters, you can set the default codec to display text. The SPS default settings for the **Telnet codec** is `500` and for the **Telnet alternate codec** is `310`.

Validating 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, but you do not have the decryption key. Click **Warnings** to see the fingerprint of the required certificate, and see Replaying encrypted audit trails to import it.
- **UPSTREAM**
  - ⊘: The upstream traffic is available and can be replayed.
  - ☒: The upstream traffic is encrypted, but you do not have the decryption key. Click **Warnings** to see the fingerprint of the required certificate, and see Replaying encrypted audit trails 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 Replaying encrypted audit trails 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 Replaying encrypted audit trails to import it.
- ?: The audit trail is not timestamped.

6

Replaying audit trails

This section describes how to replay an audit trail that is not encrypted.

To replay an encrypted audit trail, see Replaying encrypted audit trails.

You can use the SPS Search page to download an audit trail.

Prerequisites

One of the following prerequisites must be met:

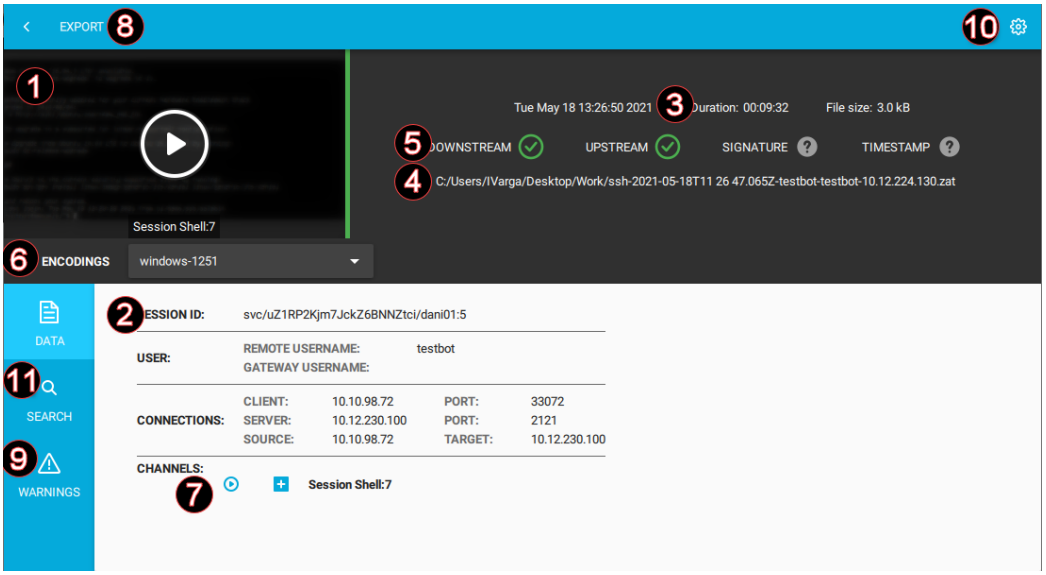
- The audit trail is available on the computer that runs the Safeguard Desktop Player.
- Using a web browser, you open the audit trail on the SPS search interface and you open the Safeguard Desktop Player application on the same computer.

To replay an unencrypted audit trail

1. Open an audit trail that you want 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 and open it.

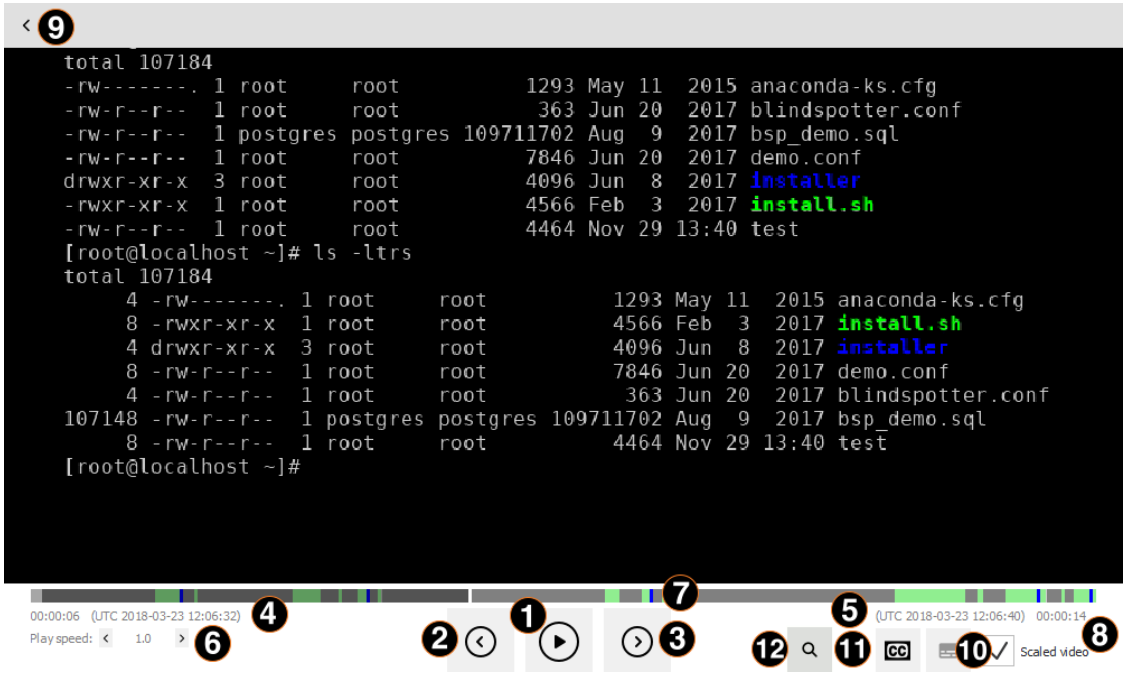
      The Safeguard Desktop Player application displays the details of the sessions stored in the audit trail file. It automatically starts to prepare (render) the audit trail for replaying. You can start replaying the audit trail while rendering is in

progress, which is useful in the case of long audit trails.



2. To start playing the audit trail, click the play button. If the audit trail contains more than one channels that can be replayed, you can select the channel to replay. Alternatively, click the ⊙ icon next to the channel that you want to replay.

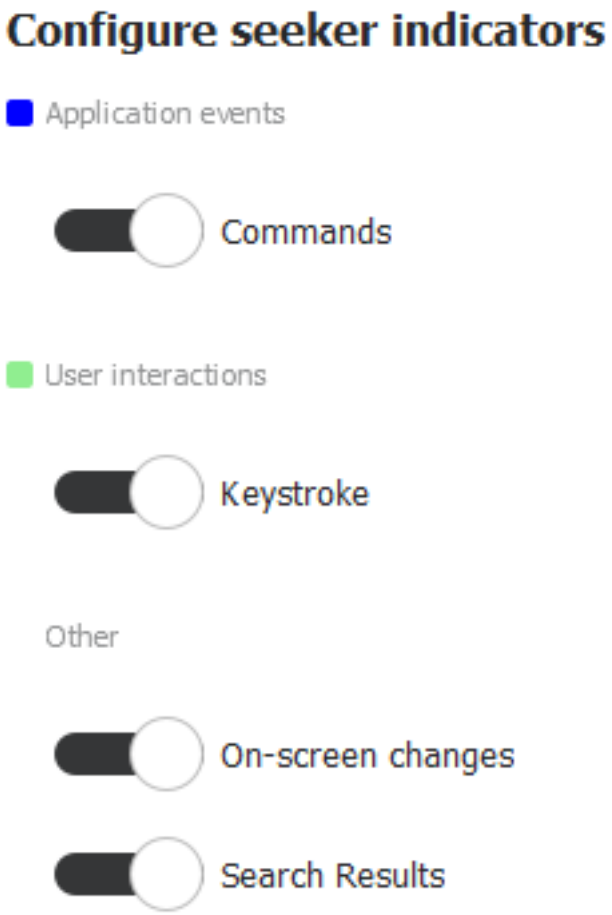
   The replay window opens.



3. To control the replay, use the following hotkeys:

- 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`
- Search in trail content: `Ctrl + F`

4. To configure the visibility of the 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 run in the session-shell channel of SSH connections, or in Telnet connections.	For terminal-based protocols	Dark blue
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

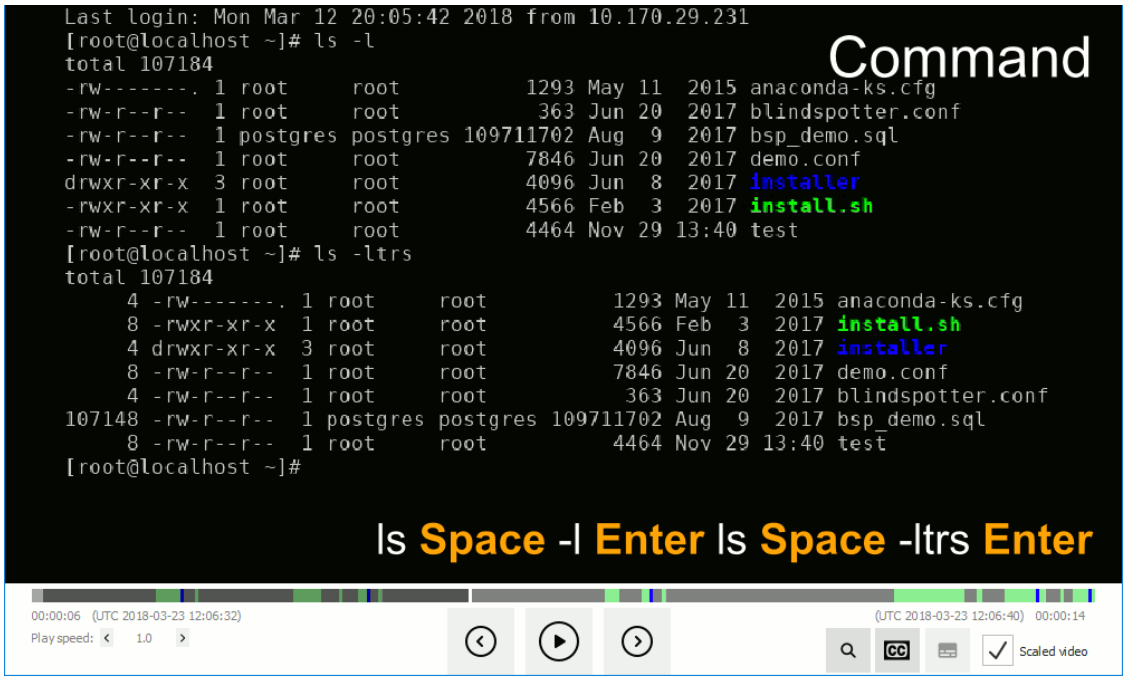
You can jump to interesting events by:

- 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 you export audit trails as video files, you can include subtitles as well. For details, see Exporting the audit trail as video.

Replaying encrypted audit trails

This section describes how to replay an encrypted audit trail. To replay encrypted audit trails using the command line, see Replaying encrypted audit trails from the command line.

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 SPS 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 SPS must be available on the host running the Safeguard Desktop Player. (This is the CA certificate of SPS 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 in PEM format, other formats are not supported.

NOTE: 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.

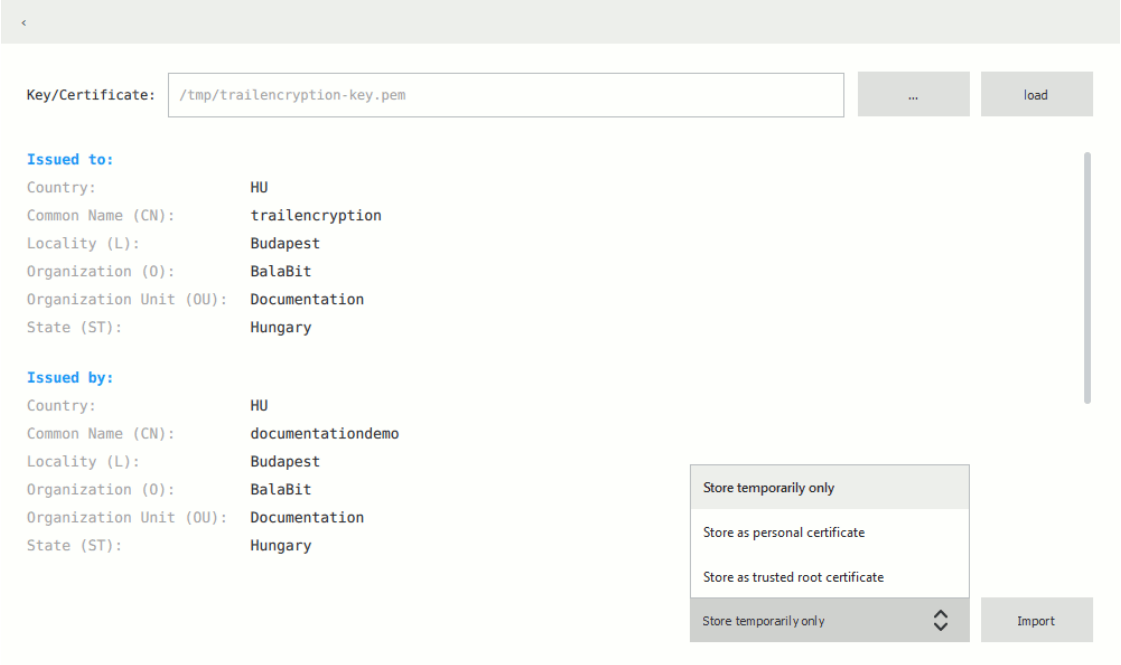
TIP: One Identity recommends using 2048-bit RSA keys (or stronger).

>

To replay an encrypted audit trail

1. Open the encrypted audit trail. Safeguard Desktop Player tries to decrypt and validate it. If the decryption or validation fails, the Safeguard Desktop Player notifies you on the screen. Click **Warnings** to see the fingerprint of the required certificate.

2. Import the required certificate. In the top-right, click ⚙ > **Key/Certificate import**.
3. Click ..., then select the certificate file. The certificates and the private keys must be available in PEM format. Other formats are not supported.



4. Click **Load**. The Safeguard Desktop Player displays the details of the certificate.
5. Select how you want to store the certificate, then click **Import**. On Microsoft Windows, you can import the certificates to the Windows Certificate Store and reuse them later. On other platforms, Safeguard Desktop Player stores the certificates only temporarily, and automatically deletes them when you close the application.
    - If you want Safeguard Desktop Player to delete the certificate after you close the application, select **Store temporarily only**.
    - If you are importing a private key to decrypt an audit trail, select **Store as personal certificate**.
    - If you are importing a CA certificate to validate the timestamp or signature of the audit trails, select **Store as trusted root certificate**.
6. Repeat the previous steps to import other certificates if needed.
7. Click ‹, then ⏵ to start replaying the audit trail.

8

Replaying encrypted audit trails from the command line

This section describes how to replay an encrypted audit trail using the command line. 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 Replaying encrypted audit trails.

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 certificates that issued the certificates used to sign the audit trail must be available and valid on the host running the Safeguard Desktop Player. (This is the certificate set at **Policies** > **Audit policies** > **Enable signing** on the SPS interface.) On Microsoft Windows, the Safeguard Desktop Player can validate this certificate from **Windows Certificate Store** > **Local Computer** > **Trusted Root Certification Authorities**.

  NOTE: In case of certificate chains, the whole chain must be imported in this Certificate Store.
- To validate timestamped audit trails, the CA certificate of SPS must be available on the host running the Safeguard Desktop Player. (This is the CA certificate of SPS 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 in PEM format, other formats are not supported.

NOTE: 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.

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

To replay an encrypted audit trail using the command line

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player.

By default, the installation directories on the different operating systems are the following:

- On Microsoft Windows platforms: `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\`
- On Linux: `~/SafeguardDesktopPlayer`
- On MacOS: `/Applications/Safeguard Desktop Player.app/Contents/Resources/`

1. (Optional) 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>
   ```

2. (Optional) 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>
   ```

3. Open the encrypted audit trail. Safeguard Desktop Player tries 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>
   ```

Replaying audit files in follow mode

This section describes how to follow active connections in semi-real time.

Prerequisites

To follow active connections, you must be allowed to authorize the sessions of the relevant connection policy. For more information on how you can configure that, see "Configuring four-eyes authorization" in the Administration Guide.

Every time you open an `.srs` file in Safeguard Desktop Player, you must authenticate yourself to SPS through Safeguard Desktop Player. To access SPS and follow active sessions, you must have:

- A valid username and password.
- The SSL certificate of your root Certificate Authority (CA).

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

On Linux or MacOS, import the SSL certificate to Safeguard Desktop Player as follows:

1. In SPS, 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 is displayed, click **PEM**. This downloads the the CA's X.509 certificate in PEM format.

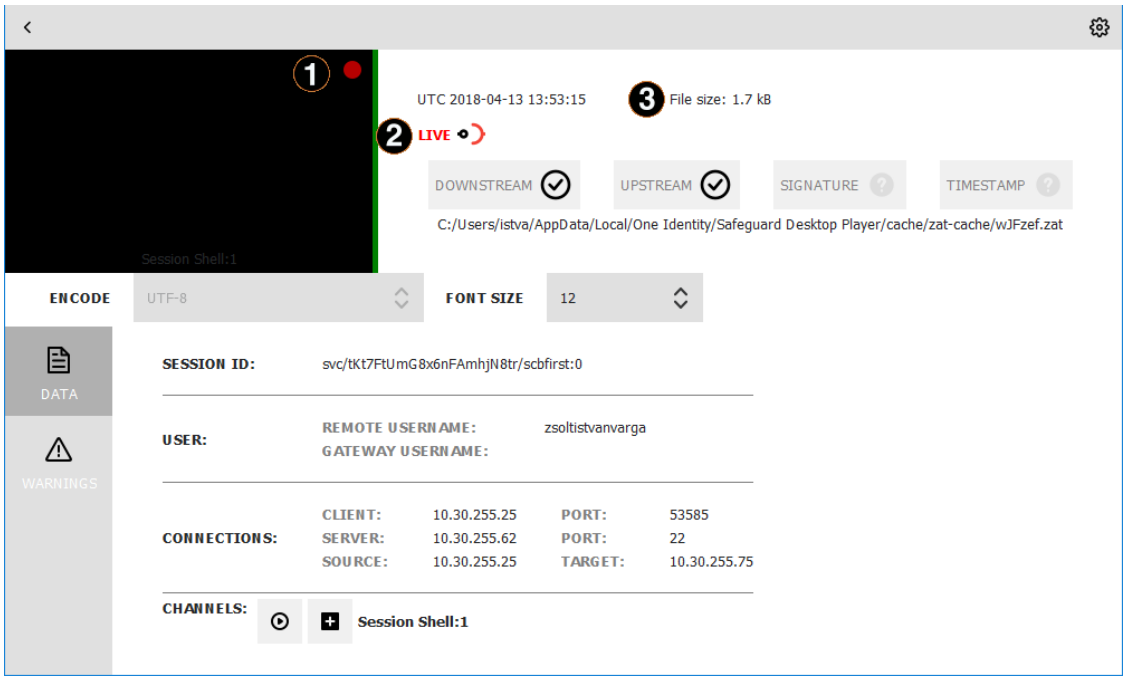
   NOTE: The certificate must be in PEM format, other formats are not supported.
4. In Safeguard Desktop Player, in the top-right, click ⚙. Select **Key/Certificate import**.
5. Click ..., then select the certificate PEM file that you downloaded from SPS.
6. Click **Load**. Safeguard Desktop Player displays the details of the certificate.
7. Click **Import**.

To follow active connections in semi-real time

1. On the SPS web interface, navigate to **Search**, select **Active** in **Connections**, and click FOLLOW next to the connection you want to monitor in semi-real time.
2. In Safeguard Desktop Player, click **OPEN**, and select the audit trail to replay.

   NOTE: If you open a closed session from an `srs` file, you can start to replay its content and follow the session even if the file has not been fully downloaded and rendered.

   Safeguard Desktop Player displays the sessions stored in the audit trail file.



   a. 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.

   b. LIVE status indicator

      The indicator shows three different states:

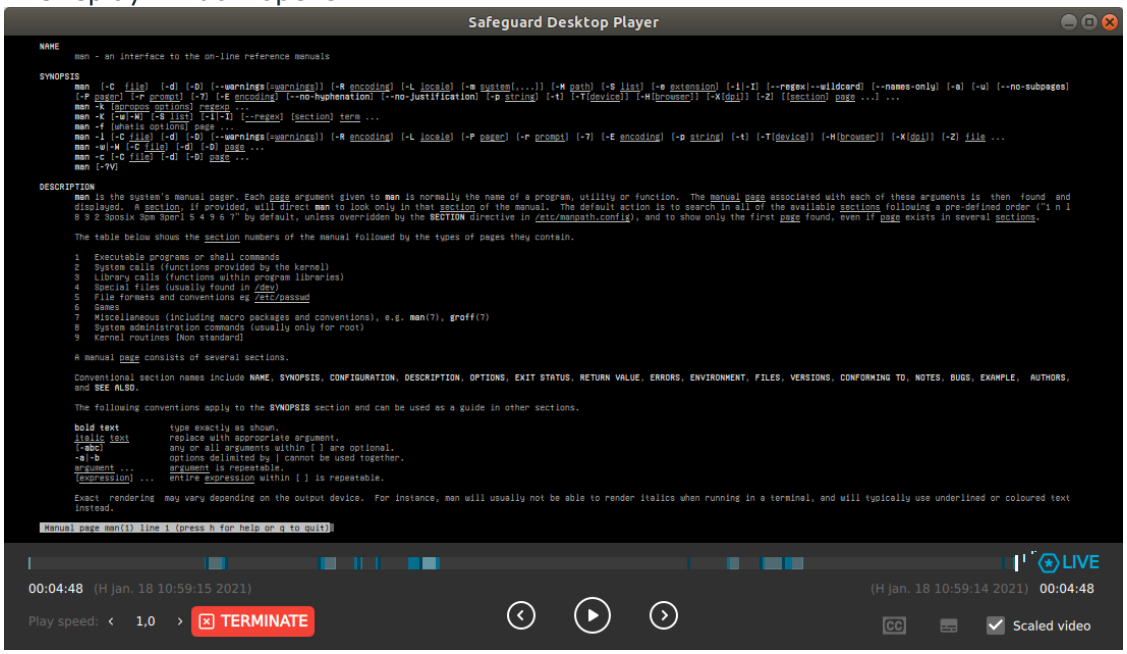
      - When it is completely red, it indicates that the connection is active and there is some user interaction on the client-side.
      - When the **LIVE** label is red but the icon is half red, half black, it indicates that the connection is active but there is no user interaction on the client-side.
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

   c. File size

It displays the size of the `.zat` file that is loaded. In the case of an active, live connection, the size continuously increases.

3. To start replaying the audit file, click the thumbnail. Alternatively, click the ⊙ icon next to the channel you want to replay.

   The replay window opens.



4.

   a. Terminate

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

   b. LIVE status indicator

      The indicator shows two different states:

      - When the Safeguard logo is animated, it indicates that the connection is active and there is some user interaction on the client-side.
      - When the Safeguard logo is static, it indicates that the connection is active but there is no user interaction on the client-side.

   The color of the **LIVE** label indicates if the displayed frame is live (blue) or an earlier frame (gray). If you stopped the playback or rewound it, to return to the live streaming, click **LIVE**.

   TIP: If 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. If you click this button, the player reverts to normal replay mode, and you can change the replay speed, and the seeker becomes available again.

TIP: You can store the `zat` or `zatx` files of sessions to replay them later without having to download them and wait for them to be rendered. For more information, see section Exporting zat and zatx files.

Searching in the content of the current audit file

Safeguard Desktop Player allows you to search in the contents of the recorded audit trails, for example, in commands that the user executed in the session, or to find a specific text that was displayed on the screen.

You can also search in the contents of the audit trails for trails of graphical sessions created and indexed with SPS 6.0.

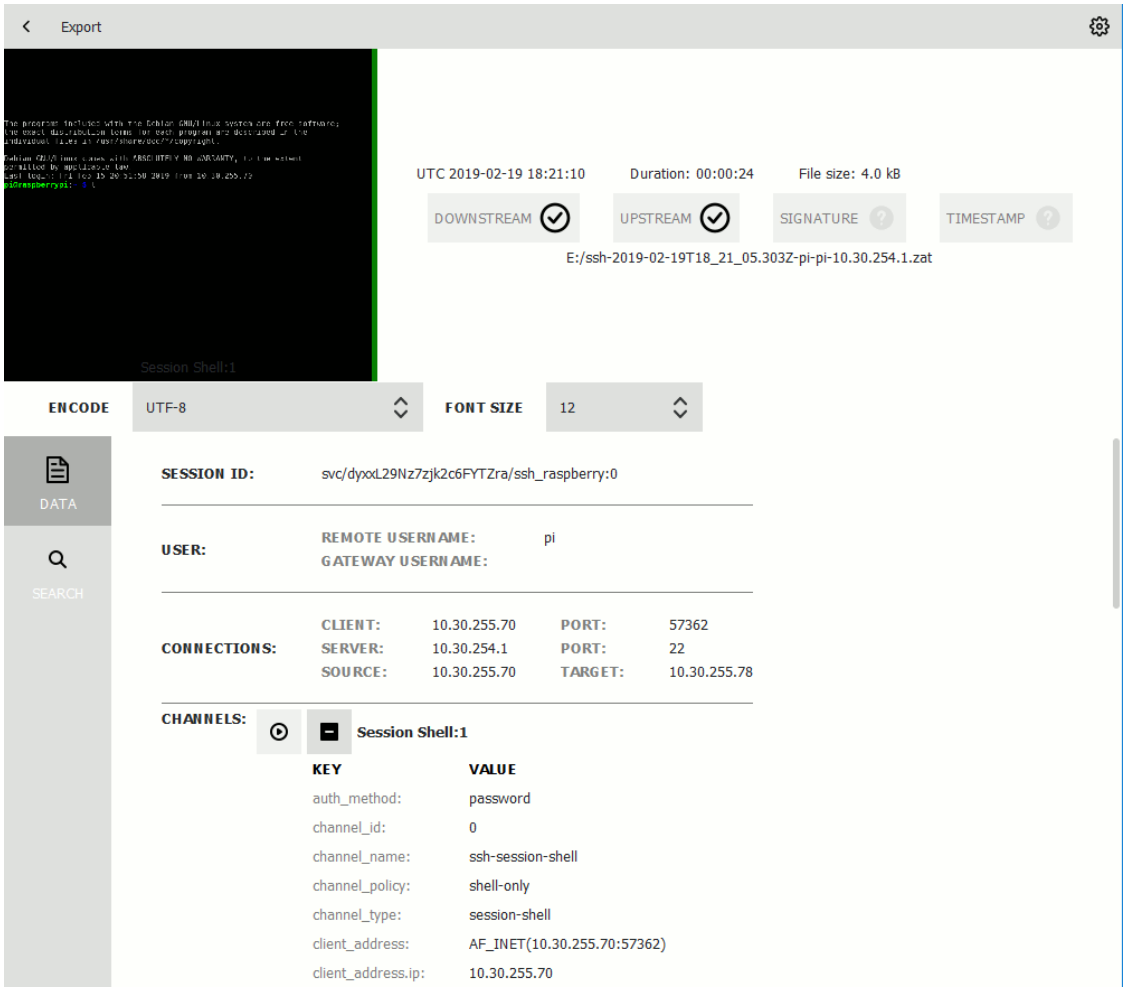
Prerequisites

- Safeguard Desktop Player version 1.7.12 or newer.
- An audit trail of a terminal session.

To search in the content of an audit file

1. In the Safeguard Desktop Player application, click **OPEN**, and select the audit trail to replay. If the audit trail is encrypted, see Replaying encrypted audit trails.

   Safeguard Desktop Player displays the sessions stored in the audit trail file.



2. Click **SEARCH** and enter your search keywords in the **Search in content** field.

   NOTE: Safeguard Desktop Player creates the index of the content when opening the file, and searching is disabled until creating the index is finished. Depending on the length of the audit trail, this can take several minutes.

   Safeguard Desktop Player displays the search results and highlights the periods of the audit trail when the search keywords were visible. For details on the search syntax, see Search query examples.

   Click ⊙ to replay the audit trail. To search while replaying an audit trail, click the magnifying glass icon.

11

Search query examples

The following sections provide examples for different search queries.

- For examples of exact matches, see Searching for exact matches on page 45.
- For examples of using boolean operators to combine search keywords, see Combining search keywords on page 46.
- For examples of wildcard searches, see Using wildcard searches on page 47.
- For examples of searching with special characters, see Searching for special characters on page 49.
- For examples of fuzzy search that finds words with similar spelling, see Searching for fuzzy matches on page 51.
- For examples of proximity search to find words that appear within a special distance, see Proximity search on page 51.
- For examples of adjusting the relevance of a search term, see Adjusting the relevance of search terms on page 51.

For details on how to use more complex keyphrases that are not covered in this guide, see the Apache Lucene documentation.

Searching for exact matches

By default, One Identity Safeguard for Privileged Sessions (SPS) searches for keywords as whole words and returns only exact matches. Note that if your search keywords include special characters, you must escape them with a backslash (\) character. For details on special characters, see Searching for special characters on page 49. The following characters are special characters: `+ - & | ! ( ) { } [ ] ^ " ~ * ? : \ /`

Example: Searching for exact matches

Search expression	`example`
Matches	example
Does not match	examples example.com query-by-example exam

To search for a string that includes a backslash characters, for example, a Windows path, use two backslashes (`\\`).

Search expression	`C\:\\Windows`
Matches	C:\Windows

Combining search keywords

You can use boolean operators – `AND`, `OR`, `NOT`, and `+` (required), – to combine search keywords. More complex search expressions can also be constructed with parentheses. If you enter multiple keywords,

Example: Combining keywords in search

Search expression	`keyword1 AND keyword2`
Matches	(returns hits that contain both keywords)

Search expression	`keyword1 OR keyword2`
Matches	(returns hits that contain at least one of the keywords)

Search expression	`keyword1 NOT keyword2`
Matches	(returns hits that contain the first phrase, but not the second)

Search expression	`+keyword1 keyword2`
Matches	(returns hits that contain keyword1, and may contain keyword2)

To search for expressions that can be interpreted as boolean operators (for example: **AND**), use the following format: **"AND"**.

Example: Using parentheses in search

Use parentheses to create more complex search expressions:

Search expression	`(keyword1 OR keyword2) AND keyword3`
Matches	(returns hits that contain either keyword1 and keyword3, or keyword2 and keyword3)

Using wildcard searches

You can use the ? and * wildcards in your search expressions.

Example: Using wildcard ? in search

The ? (question mark) wildcard means exactly one arbitrary character. Note that it does not work for finding non-UTF-8 or multibyte characters. If you want to search for these characters, the expression ?? might work, or you can use the * wildcard instead.

You cannot use a * or ? symbol as the first character of a search.

Search expression	`example?`
Matches	example1 examples example?
Does not match	example.com

	example12 query-by-example
Search expression	`example??`
Matches	example12
Does not match	example.com example1 query-by-example

Example: Using wildcard * in search

The * wildcard means 0 or more arbitrary characters. It finds non-UTF-8 and multibyte characters as well.

Search expression	`example*`
Matches	example examples example.com
Does not match	query-by-example example*

Example: Using combined wildcards in search

Wildcard characters can be combined.

Search expression	`ex?mple*`
Matches	example1 examples example.com exemple.com

	example12
Does not match	exmples query-by-example

Searching for special characters

To search for the special characters, for example, question mark (?), asterisk (*), backslash (\) or whitespace ( ) characters, you must prefix these characters with a backslash (\). Any character after a backslash is handled as character to be searched for. The following characters are special characters: `+ - & | ! ( ) { } [ ] ^ " ~ * ? : \ /`

Example: Searching for special characters

To search for a special character, use a backslash (\).

Search expression	`example\?`
Matches	example?
Does not match	examples example1

To search for a string that includes a backslash characters, for example, a Windows path, use two backslashes (\\).

Search expression	`C\:\\Windows`
Matches	C:\Windows

To search for a string that includes a slash character, for example, a UNIX path, you must escape the every slash with a backslash (\/).

Search expression	`\/var\/log\/messages`
Matches	/var/log/messages

Search expression	`\(1\+1\)\:2`
Matches	(1+1):2

Searching in commands and window titles

For terminal connections, use the `command:` prefix to search only in the commands (excluding screen content). For graphical connections, use the `title:` prefix to search only in the window titles (excluding screen content). To exclude search results that are commands or window titles, use the following format: `keyword AND NOT title:[* TO *]`.

You can also combine these search queries with other expressions and wildcards, for example, `title:properties AND gateway`.

Example: Searching in commands and window titles

Search expression	`command:sudo su`
Matches	`sudo su` as a terminal command
Does not match	`sudo su` in general screen content

Search expression	`title:settings`
Matches	`settings` appearing in the title of an active window
Does not match	`settings` in general screen content

To find an expression in the screen content and exclude search results from the commands or window titles, see the following example.

Search expression	`properties AND NOT title:[* TO *]`
Matches	`properties` appearing in the screen content, but not as a window title.
Does not match	`properties` in window titles.

You can also combine these search filters with other expressions and wildcards.

Search expression	`title:properties AND gateway`
Matches	A screen where `properties` appears in the window title, and `gateway` in the screen content (or as part of the window title).
Does not match	Screens where both `properties` and `gateway` appear, but `properties` is not in the window title.

Searching for fuzzy matches

Fuzzy search uses the tilde ~ symbol at the end of a single keyword to find hits that contain words with similar spelling to the keyword.

Example: Searching for fuzzy matches

Search expression	`roam~`
Matches	roams foam

Proximity search

Proximity search uses the tilde ~ symbol at the end of a phrase to find keywords from the phrase that are within the specified distance from each other.

Example: Proximity search

Search expression	`keyword1 keyword2 ~10`
Matches	(returns hits that contain keyword1 and keyword2 within 10 words from each other)

Adjusting the relevance of search terms

By default, every keyword or phrase of a search expression is treated as equal. Use the caret ^ symbol to make a keyword or expression more important than the others.

Example: Adjusting the relevance of search terms

Search expression	`keyword1^4 keyword2`
Matches	(returns hits that contain keyword1 and keyword2, but keyword1 is 4-times more relevant)

Search expression	`keyword1^5 keyword2`
Matches	(returns hits that contain keyword1 and keyword2, but keyword1 is 5-times more relevant)

Exporting the audit trail as video

This section describes how to export an audit trail as a video file (optionally, including the accompanying subtitles).

NOTE: To export an audit trail, you must open it.

The exported files use the WEBM format with the VP8 codec. You can replay WebM videos in most modern browsers, and several media player applications. For details, see the Playing WebM Video page.

Prerequisites

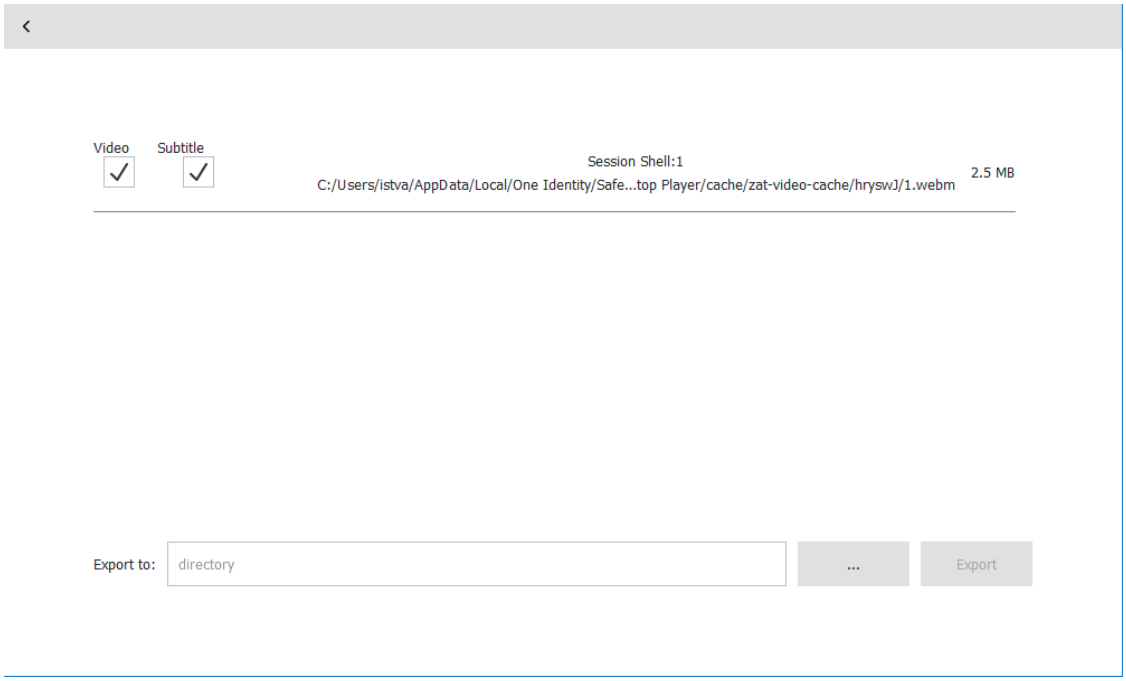
To use Internet Explorer, you must install an add-on.

To export an audit trail as a video file

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 Replaying encrypted audit trails.
2. Click **EXPORT** > **Export video**.
3. If the audit trail contains multiple channels that can be replayed, select which channels you want to export.
4. To export the subtitles listing the user events that occurred in the session (window titles that appeared on the screen, commands executed, mouse activity, and keystrokes), select the **Subtitle** checkbox.

Figure 13: Export options



5. Click ..., and select the directory where you want to save the video file.
6. Click **EXPORT**.

Exporting the sound from an audit trail

You can enable auditing the sound that is transferred between an RDP client and the server. Using the **Export audio** option of Safeguard Desktop Player, you can export the input sound (the one that comes from the audited user) and the output sound (the one that is received by the audited user) into **.wav** files.

Prerequisites

In SPS, using the **Channel Policies** settings of the **RDP Control** option, select the **Record audit trail** checkbox for the **Sound** and the **Dynamic virtual channel** in the policy that you want to use for sound auditing.

For more information, see Configuring SPS to enable exporting sound from audit trails in the SPS *Administration Guide*.

To export the sound from an audit trail

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 Replaying encrypted audit trails.
2. Click the **EXPORT** > **Export audio...** button.
3. In the **Select folder** window, navigate to the folder where you want to save the exported sound files of the audit trail.

The displayed dialog shows the exported files with their paths. On clicking the paths, the destination folders open. The dialog also lists the errors that occurred during the export. The sound files are saved in the following format:

- `<timestamp>_input.wav`
- `<timestamp>_output.wav`

Exporting zat and zatx files

Using the **Export zat/zatx...** option of Safeguard Desktop Player, you can save the trail currently opened to a selected location.

After opening an `srs` file, you can export its content to a `zat` or `zatx` file if all the following criteria are met:

- The `srs` file does not belong to a live stream.
- Safeguard Desktop Player has fully downloaded the content of the `srs` file.
- You can replay the content of the `srs` file.

To export `zat` or `zatx` files from an audit trail

1. Open the audit trail in Safeguard Desktop Player.

   If the audit trail is encrypted, you need the appropriate decryption keys to open it. For more information, see Replaying encrypted audit trails.
2. Select **EXPORT** > **Export zat/zatx...**.
3. In the **Select folder** window, navigate to the folder where you want to save the exported `zat` or `zatx` files of the audit trail.

The displayed dialog shows the exported file with the `trail.zat` or `trail.zatx` file name.

Sharing an encrypted audit trail

This section describes how to share an encrypted audit trail with a third party.

NOTE: To export an audit trail, you must open 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 only do this by 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.

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

To share an encrypted audit trail with a third party

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player.

By default, the installation directories on the different operating systems are the following:

- On Microsoft Windows platforms: `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\`
- On Linux: `~/SafeguardDesktopPlayer`
- On MacOS: `/Applications/Safeguard Desktop Player.app/Contents/Resources/`

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 or MacOS: `./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:

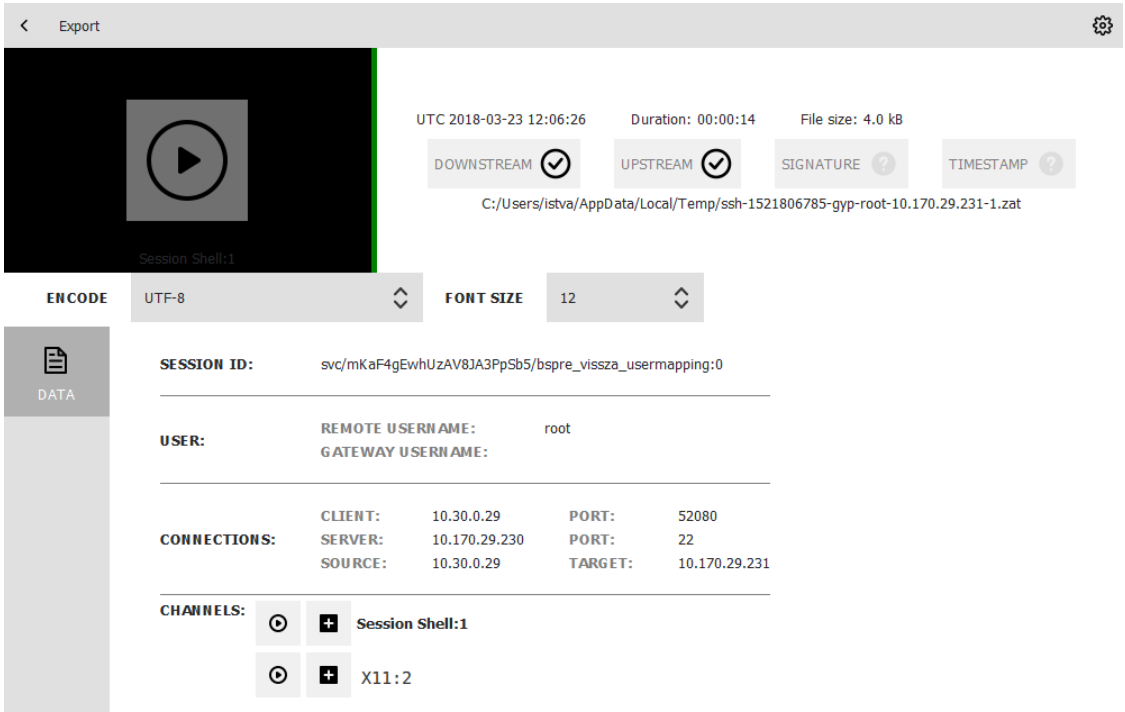
```
./adp --task rekey --file /tmp/ssh-171128T1353-frobert-frobert-10.30.255.68.zat --key /tmp/indexer-certificate-key.pem: --out /tmp/shared-ssh.zat --new-cert /tmp/new-encryption-certificate.pem
```

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 SPS application.

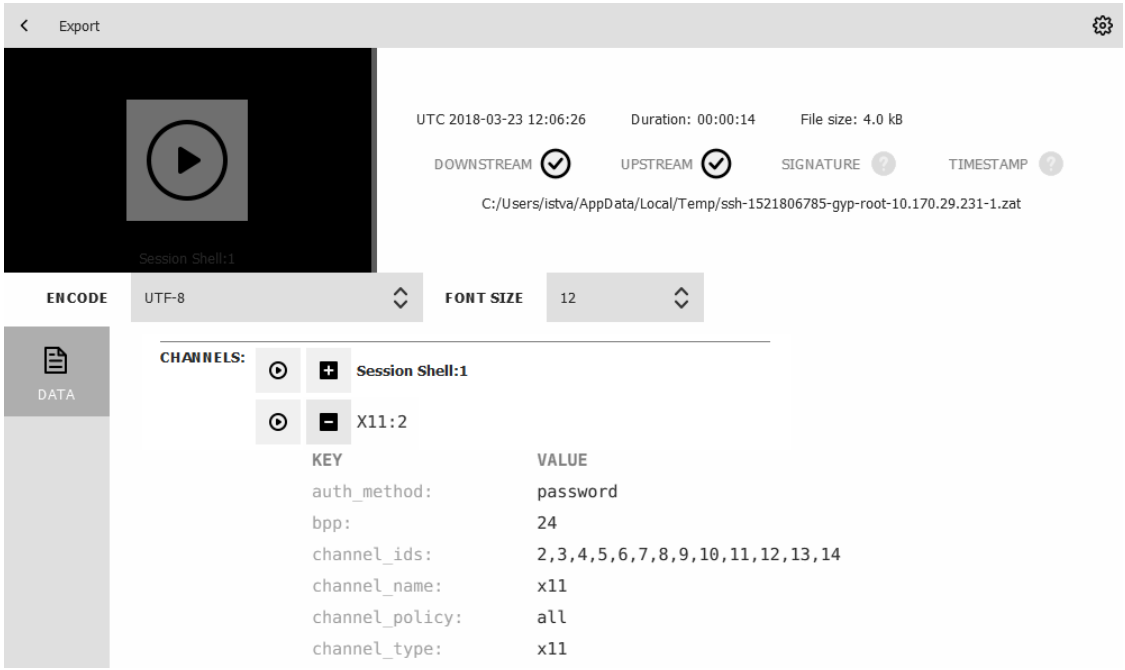
Replaying X11 sessions

With the Safeguard Desktop Player application, you 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 consider 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.

15

Exporting transferred files from SCP, SFTP, HTTP, and RDP audit trails

You can export the files that the user transferred in SCP, SFTP, and HTTP sessions as well as through the RDP clipboard. You can export such files from the audit trails using the command line or the Safeguard Desktop Player GUI.

NOTE: Exporting transferred files through the RDP clipboard is a feature that has been tested with Microsoft-supported clients.

Exporting files from an audit trail after RDP file transfer through clipboard or disk redirection

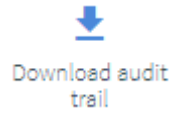
Prerequisites

Configure SPS to allow exporting files from an audit trail. For more information, see Configuring SPS to enable exporting files from audit trails after RDP file transfer.

NOTE: By default, the Safeguard Desktop Player application only exports complete files. To export partially transferred files, see Exporting transferred files from SCP, SFTP, HTTP and RDP audit trail using the command line.

To export files from an audit trail after RDP file transfer through clipboard or disk redirection

1. Navigate to **Main Menu** > **Search** in SPS, select the session during which the files were copy-pasted through the clipboard or transferred through disk redirection, and click ••• .

2. Click 

, save the .zat file, and open the Safeguard Desktop Player application.
3. Open the `.zat` file and click  in the Safeguard Desktop Player interface window.
4. Navigate to **EXPORT** > **Export transferred files...** and select **Choose** in the **Select folder – Safeguard Desktop Player** window. Safeguard Desktop Player automatically displays the files in a new window under **EXPORTED FILES (<number of files>)**, with information about the files' original path.
5. (Optional) Open the files to see if the export was successful.

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

This section describes how to export the files that you transferred, using the command line, in one of the following sessions:

- SCP
- SFTP
- HTTP
- RDP

To export the files that you transferred in an SCP, SFTP, HTTP, or RDP session using the command line

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player.

By default, the installation directories on the different operating systems are the following:

- On Microsoft Windows platforms: `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\`
- On Linux: `~/SafeguardDesktopPlayer`
- On MacOS: `/Applications/Safeguard Desktop Player.app/Contents/Resources/`

NOTE: By default, the Desktop Player only exports complete files. If you want to export partially transferred files as well, use the `adp --export-files` command.

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 or MacOS: `./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 --task indexer --channel 3 --file <path/to/audit-trail.zat> --export-files <folder/to/save/files/>`

   Linux or MacOS: `adp --task indexer --channel 3 --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.

16

Exporting 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.

Exporting raw network traffic in PCAP format using the command line

This section describes how to export raw network traffic in PCAP format using the command line.

To export raw network traffic in PCAP format using the command line

Start a command prompt and navigate to the installation directory of Safeguard Desktop Player.

By default, the installation directories on the different operating systems are the following:

- On Microsoft Windows platforms: `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\`
- On Linux: `~/SafeguardDesktopPlayer`
- On MacOS: `/Applications/Safeguard Desktop Player.app/Contents/Resources/`

1. List the channels in the audit trail, and find the ones that you want to export. Note down the ID number of the channels 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 or MacOS: `./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 channels from the audit trail. Use the ID numbers of the channels from the previous step.
   - Windows: `adp.exe -f <path/to/audit-trail.zat> -c <channel id> -t indexer --export-pcap output.pcap`
   - Linux or MacOS: `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.

Exporting raw network traffic in PCAP format using the GUI

This section describes how to export the channels stored in the audit trail using the GUI.

To export the channels stored in the audit trail using the GUI

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 Replaying encrypted audit trails.
2. Click **EXPORT** > **Export pcap**.

   The **Select folder** dialog pops up.
3. Select the directory where you want to save the files. Click **Choose**.

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

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

Exporting screen content text

This section describes how to export screen content text from text-based protocols (terminal-based protocols and HTTP) in TXT format. Screen content text is saved into files as UTF-8 encoded text with UNIX timestamps.

To export screen content text from text-based protocols (terminal-based protocols and HTTP) in TXT format

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 Replaying encrypted audit trails.

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

   The **Select folder** dialog pops up.

3. Select the directory where you want to save the files. Click **Choose**.

   Once the export process is finished, a **FILES** dialog pops up, indicating the number of exported files 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

18

Troubleshooting the Safeguard Desktop Player

Determining 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`

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

The following describes how to export the files that the user transferred in an SCP, SFTP, or HTTP session using the GUI.

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

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 Replaying encrypted audit trails.
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.

.zat, .zatx, and .srs files not opened automatically

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

Problems in VirtualBox

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

If these do not solve the problem, see Force rendering software.

Force rendering software

Some video card drivers might have problems 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 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

On Microsoft Windows, you cannot import CA certificates from a shared drive.

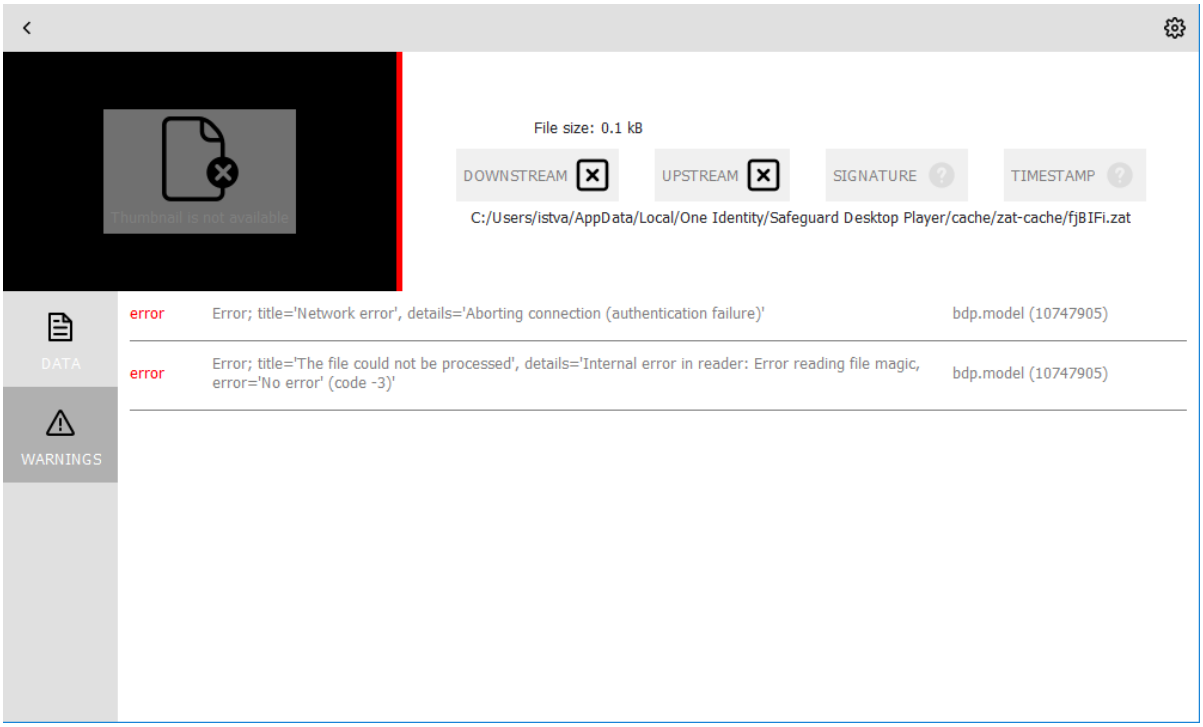
Copy the certificate to a local folder and import it from there.

Also, you must install the Safeguard Desktop Player application 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 14: Warnings and logs



To specify the log level of the Safeguard Desktop Player application, use the following command-line parameters.

- `-l` or `--log-level` <number>
- Set the log level of Safeguard Desktop Player:
  - `3` - Default log level.
  - `0` - Completely disables logging.
  - `7` - The is most verbose level, 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"`

19

Keyboard shortcuts

You can use the following keyboard shortcuts 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`
- Search in trail content: `Ctrl + F`

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 and other inquiries, such as licensing, support, and renewals, visit https://www.oneidentity.com/company/contact-us.aspx.

Technical support resources

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

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

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