One Identity Safeguard for Privileged Sessions 6.0

Safeguard Desktop Player User Guide

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

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

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

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

Patents

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

Trademarks

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

Legend

⊗ **WARNING: A WARNING icon 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.**

SPS Safeguard Desktop Player User Guide
Updated - July 2019
Version - 6.0

Contents

1

Summary of changes

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 Search 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 Install 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 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.

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, Mac
Can replay audit trails recorded with SPS 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 display user input	✔	✔
Can display subtitles for video	-	✔
Export audit trail as video	-	✔
Export screen content text	-	✔
Can search in the contents of the audit trails	-	✔

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

⚠ **CAUTION:**

Starting with SPS 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 SPS 5 F4 and later.

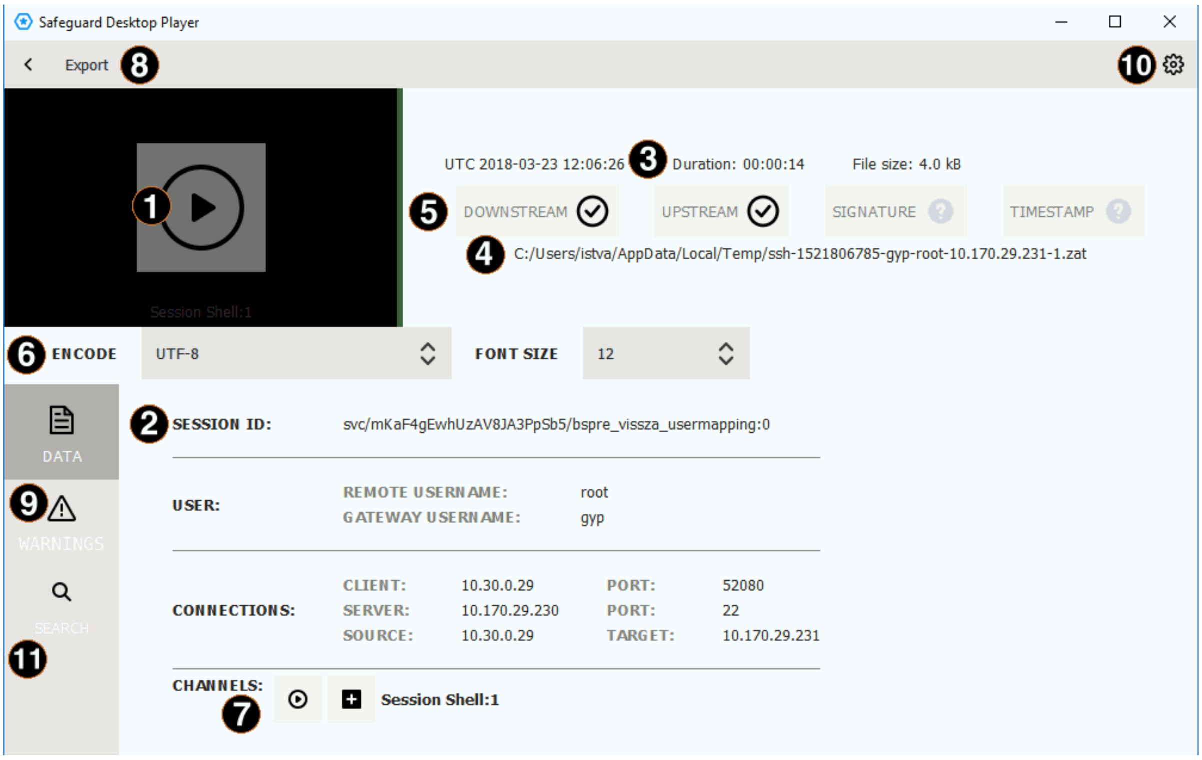
3

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). 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



UTC 2018-03-23 12:06:26 Duration: 00:00:14 File size: 4.0 kB

C:/Users/istva/AppData/Local/Temp/ssh-1521806785-gyp-root-10.170.29.231-1.zat

ENCODE UTF-8 FONT SIZE 12

SESSION ID: svc/mKaF4gEwhUzAV8JA3PpSb5/bspre_vissza_usermapping:0

USER:	REMOTE USERNAME:	root		
	GATEWAY USERNAME:	gyp		
CONNECTIONS:	CLIENT:	10.30.0.29	PORT:	52080
	SERVER:	10.170.29.230	PORT:	22
	SOURCE:	10.30.0.29	TARGET:	10.170.29.231

CHANNELS: Session Shell:1

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" 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 "Searching audit trails: the One Identity Safeguard for Privileged Sessions (SPS) 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**

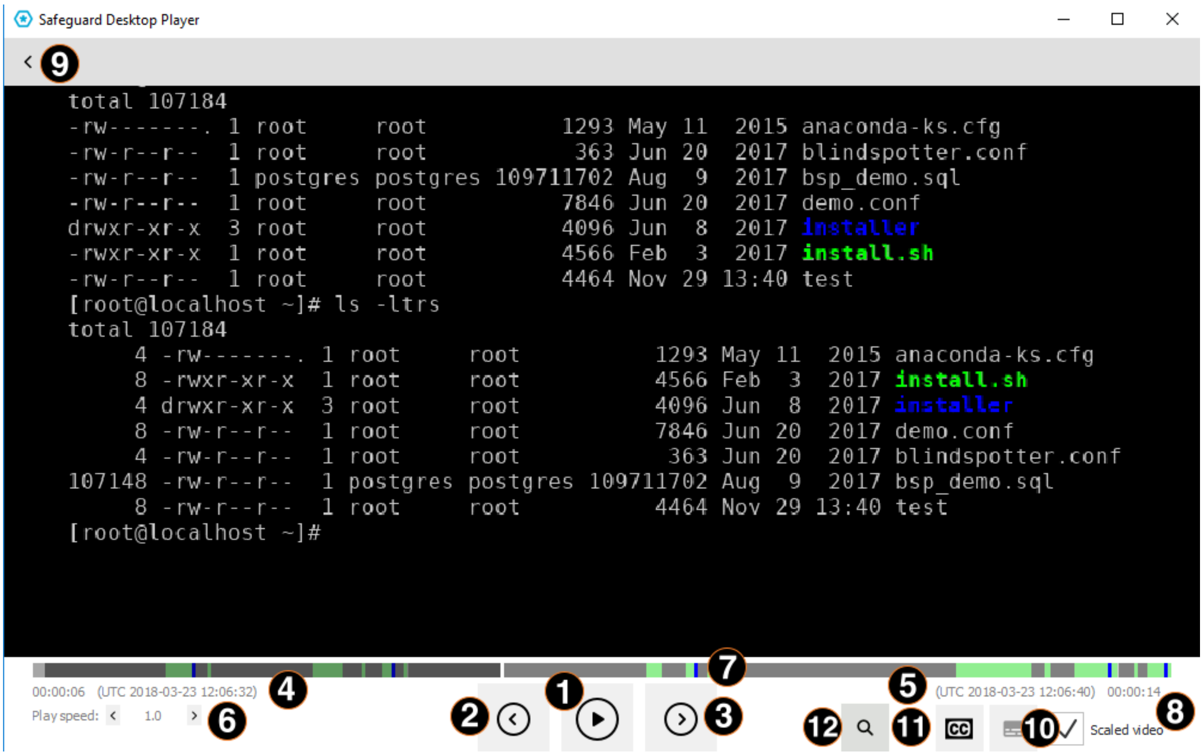
   Warnings and errors that occurred during opening and processing the audit trail file.

10. **Help**

    Open the documentation in your browser.

11. **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. Available only for terminal sessions. For details, see Search in the content of the current audit file.



```
total 107184
-rw-------. 1 root     root          1293 May 11  2015 anaconda-ks.cfg
-rw-r--r--  1 root     root           363 Jun 20  2017 blindspotter.conf
-rw-r--r--  1 postgres postgres 109711702 Aug  9  2017 bsp_demo.sql
-rw-r--r--  1 root     root          7846 Jun 20  2017 demo.conf
drwxr-xr-x  3 root     root          4096 Jun  8  2017 installer
-rwxr-xr-x  1 root     root          4566 Feb  3  2017 install.sh
-rw-r--r--  1 root     root          4464 Nov 29 13:40 test
[root@localhost ~]# ls -ltrs
total 107184
     4 -rw-------. 1 root     root          1293 May 11  2015 anaconda-ks.cfg
     8 -rwxr-xr-x  1 root     root          4566 Feb  3  2017 install.sh
     4 drwxr-xr-x  3 root     root          4096 Jun  8  2017 installer
     8 -rw-r--r--  1 root     root          7846 Jun 20  2017 demo.conf
     4 -rw-r--r--  1 root     root           363 Jun 20  2017 blindspotter.conf
107148 -rw-r--r--  1 postgres postgres 109711702 Aug  9  2017 bsp_demo.sql
     8 -rw-r--r--  1 root     root          4464 Nov 29 13:40 test
[root@localhost ~]#
```

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.

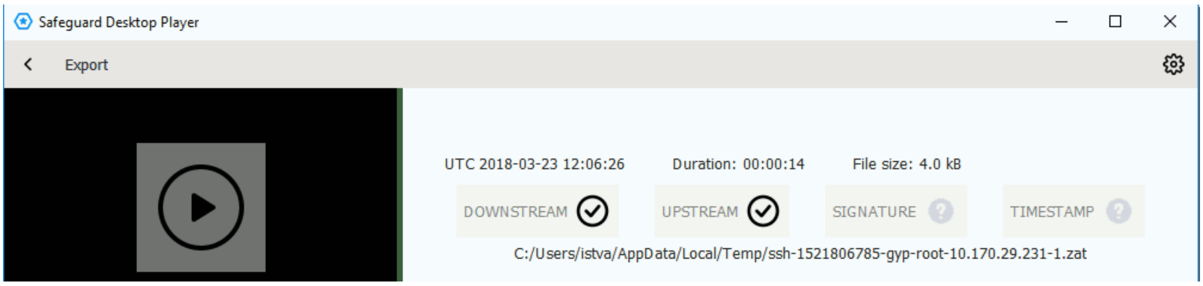
12. **Search in trail content**

    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. Available only for terminal sessions. For details, see Search in the content of the current audit file.

4

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.



Safeguard Desktop Player

Export

UTC 2018-03-23 12:06:26 Duration: 00:00:14 File size: 4.0 kB

DOWNSTREAM ✓ UPSTREAM ✓ SIGNATURE ? TIMESTAMP ?

C:/Users/istva/AppData/Local/Temp/ssh-1521806785-gyp-root-10.170.29.231-1.zat

- ✓ 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 Replay encrypted audit trails 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 Replay 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 Replay 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 Replay encrypted audit trails to import it.
- ?: The audit trail is not timestamped.

Replay audit trails

The following describes how to replay an unencrypted audit trail.

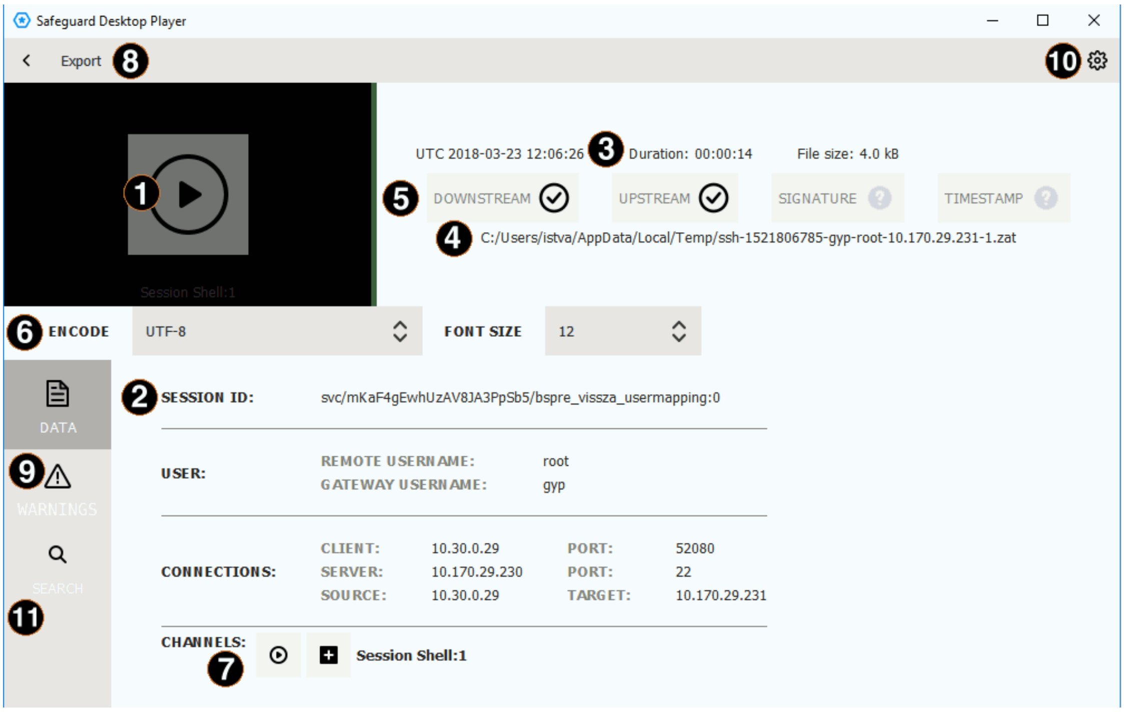
To replay an encrypted audit trail, see Replay encrypted audit trails.

Prerequisites:

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

To replay an unencrypted audit trail

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.



UTC 2018-03-23 12:06:26 Duration: 00:00:14 File size: 4.0 kB

C:/Users/istva/AppData/Local/Temp/ssh-1521806785-gyp-root-10.170.29.231-1.zat

ENCODE: UTF-8 FONT SIZE: 12

SESSION ID: svc/mKaF4gEwhUzAV8JA3PpSb5/bspre_vissza_usermapping:0

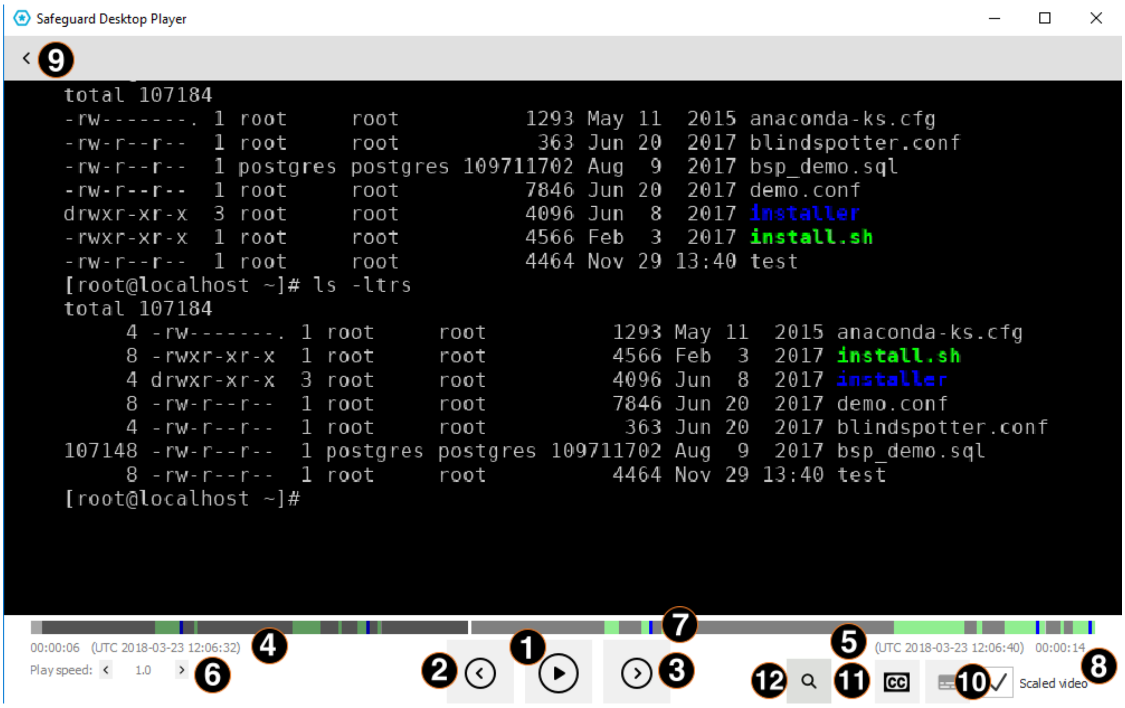
USER: REMOTE USERNAME: root
GATEWAY USERNAME: gyp

CONNECTIONS:				
	CLIENT:	10.30.0.29	PORT:	52080
	SERVER:	10.170.29.230	PORT:	22
	SOURCE:	10.30.0.29	TARGET:	10.170.29.231

CHANNELS: Session Shell:1

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.



```
total 107184
-rw-------. 1 root     root          1293 May 11  2015 anaconda-ks.cfg
-rw-r--r--  1 root     root           363 Jun 20  2017 blindspotter.conf
-rw-r--r--  1 postgres postgres 109711702 Aug  9  2017 bsp_demo.sql
-rw-r--r--  1 root     root          7846 Jun 20  2017 demo.conf
drwxr-xr-x  3 root     root          4096 Jun  8  2017 installer
-rwxr-xr-x  1 root     root          4566 Feb  3  2017 install.sh
-rw-r--r--  1 root     root          4464 Nov 29 13:40 test
[root@localhost ~]# ls -ltrs
total 107184
     4 -rw-------. 1 root     root          1293 May 11  2015 anaconda-ks.cfg
     8 -rwxr-xr-x  1 root     root          4566 Feb  3  2017 install.sh
     4 drwxr-xr-x  3 root     root          4096 Jun  8  2017 installer
     8 -rw-r--r--  1 root     root          7846 Jun 20  2017 demo.conf
     4 -rw-r--r--  1 root     root           363 Jun 20  2017 blindspotter.conf
107148 -rw-r--r--  1 postgres postgres 109711702 Aug  9  2017 bsp_demo.sql
     8 -rw-r--r--  1 root     root          4464 Nov 29 13:40 test
[root@localhost ~]#
```

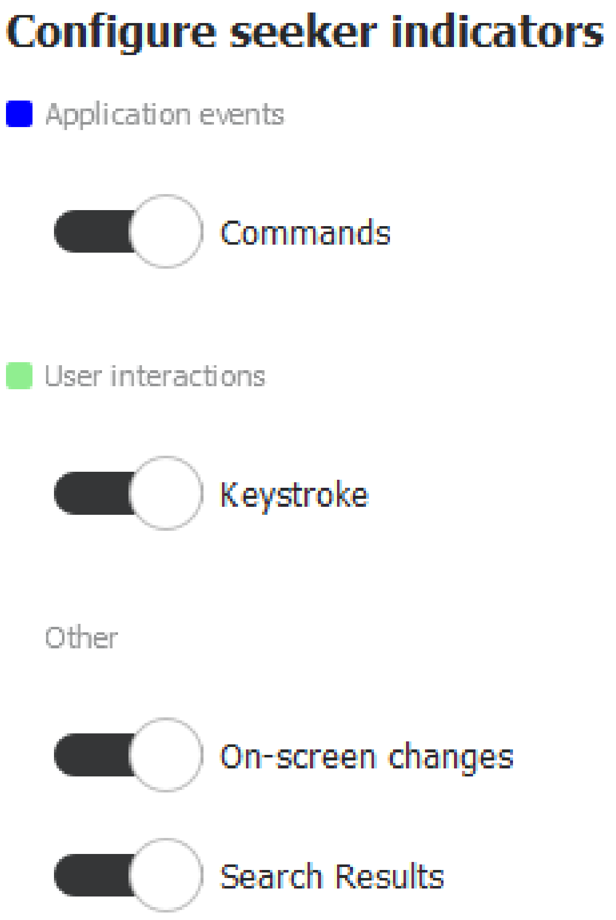
00:00:06 (UTC 2018-03-23 12:06:32) (UTC 2018-03-23 12:06:40) 00:00:14

Play speed: ‹ 1.0 ›

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

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



Configure seeker indicators

🟦 Application events

Commands: ● on

🟩 User interactions

Keystroke: ● on

Other

On-screen changes: ● on

Search Results: ● on

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 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

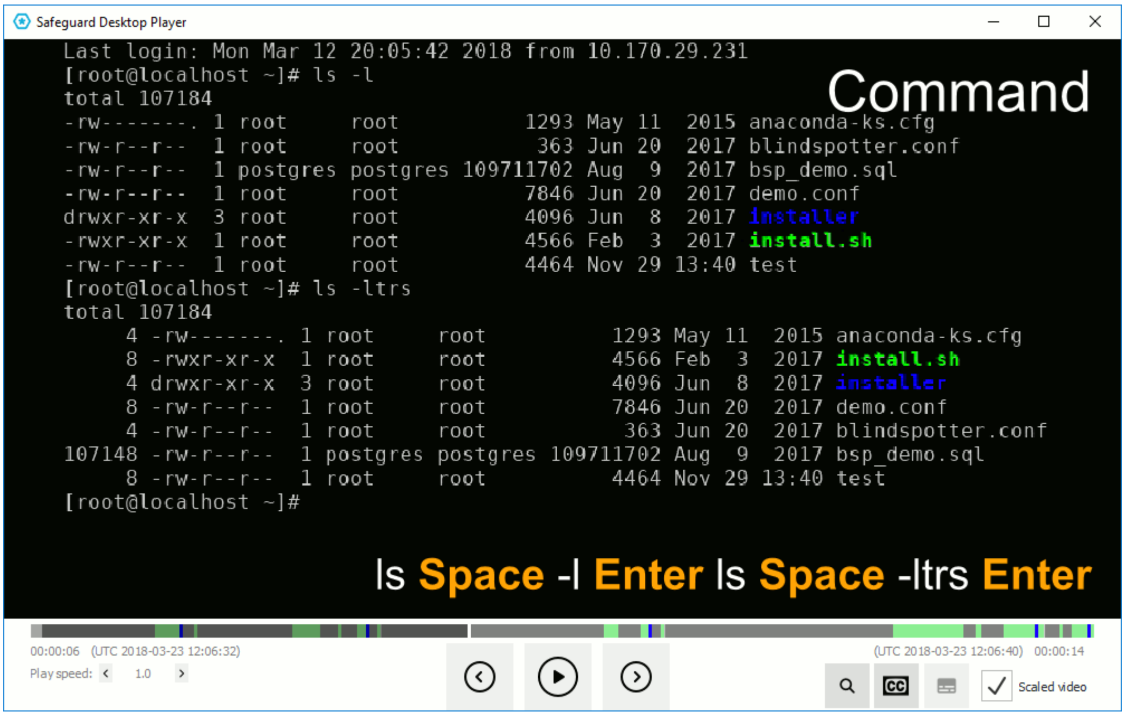
You can jump to interesting events by:

- 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.



Safeguard Desktop Player
Command
ls Space -l Enter ls Space -ltrs Enter
00:00:06 (UTC 2018-03-23 12:06:32)
Play speed: ‹ 1.0 ›
(UTC 2018-03-23 12:06:40) 00:00:14
CC
Scaled video

```
Last login: Mon Mar 12 20:05:42 2018 from 10.170.29.231
[root@localhost ~]# ls -l
total 107184
-rw-------. 1 root     root          1293 May 11  2015 anaconda-ks.cfg
-rw-r--r--  1 root     root           363 Jun 20  2017 blindspotter.conf
-rw-r--r--  1 postgres postgres 109711702 Aug  9  2017 bsp_demo.sql
-rw-r--r--  1 root     root          7846 Jun 20  2017 demo.conf
drwxr-xr-x  3 root     root          4096 Jun  8  2017 installer
-rwxr-xr-x  1 root     root          4566 Feb  3  2017 install.sh
-rw-r--r--  1 root     root          4464 Nov 29 13:40 test
[root@localhost ~]# ls -ltrs
total 107184
     4 -rw-------. 1 root     root          1293 May 11  2015 anaconda-ks.cfg
     8 -rwxr-xr-x  1 root     root          4566 Feb  3  2017 install.sh
     4 drwxr-xr-x  3 root     root          4096 Jun  8  2017 installer
     8 -rw-r--r--  1 root     root          7846 Jun 20  2017 demo.conf
     4 -rw-r--r--  1 root     root           363 Jun 20  2017 blindspotter.conf
107148 -rw-r--r--  1 postgres postgres 109711702 Aug  9  2017 bsp_demo.sql
     8 -rw-r--r--  1 root     root          4464 Nov 29 13:40 test
[root@localhost ~]#
```

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

6

Replay encrypted audit trails

⚠ **CAUTION:**

> **Starting with SPS 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 SPS 5 F4 and later.**

The following describes how to replay an encrypted audit trail. To replay encrypted audit trails using the command line, see Replay 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 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.

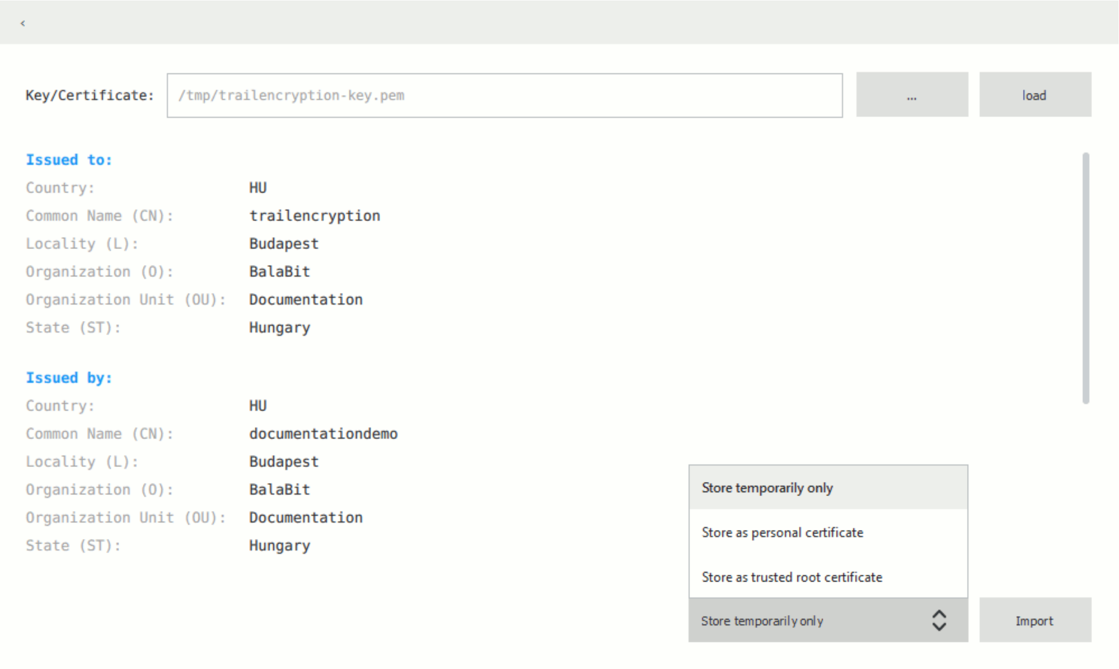
NOTE:

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).

To replay an encrypted audit trail

1. Open the encrypted audit trail. The Safeguard Desktop Player will attempt 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. At the top, on the right, click ⚙ **> Key/Certificate import**.
3. Click …, then select the certificate file. The certificates and the private keys must be available as a file in PEM format. Other formats are not supported.



Key/Certificate: /tmp/trailencryption-key.pem

Issued to:

Country:	HU
Common Name (CN):	trailencryption
Locality (L):	Budapest
Organization (O):	BalaBit
Organization Unit (OU):	Documentation
State (ST):	Hungary

Issued by:

Country:	HU
Common Name (CN):	documentationdemo
Locality (L):	Budapest
Organization (O):	BalaBit
Organization Unit (OU):	Documentation
State (ST):	Hungary

Store temporarily only

...
load
Store temporarily only
Store as personal certificate
Store as trusted root certificate
Import

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 into 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.

Replay encrypted audit trails from the command line

⚠ **CAUTION:**

Starting with SPS 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 SPS 5 F4 and later.

The following 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 Replay 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 that 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 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).

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

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>
   ```

8

Replay audit files in follow mode

> ⚠ **CAUTION:**
>
> **Starting with SPS 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 SPS 5 F4 and later.**

The following describes how to follow active connections in semi-real time.

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 "Configuring four-eyes authorization" in the Administration Guide.

Every time you open an `.srs` file in Safeguard Desktop Player for replay, you are required to authenticate yourself to SPS through the user interface of Safeguard Desktop Player. To be able 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, the 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 by completing the following steps:

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 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

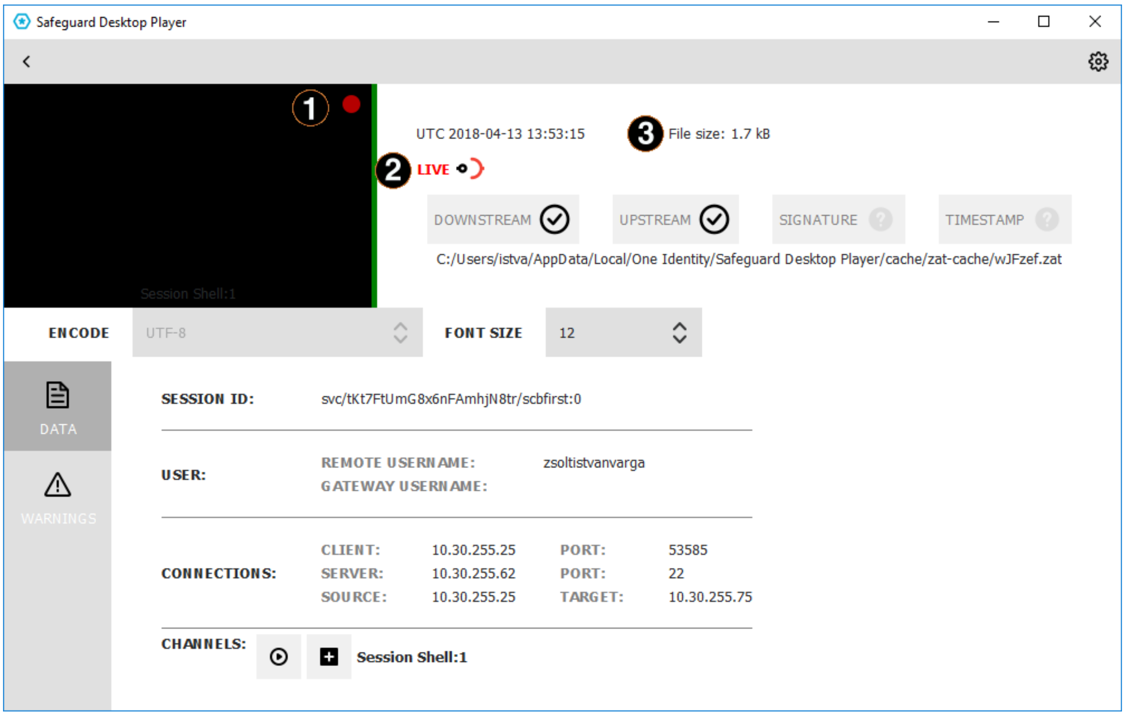
Key/Certificate import.

5. Click ..., then select the certificate PEM file that you downloaded from SPS.
6. Click **Load**. The Safeguard Desktop Player displays the details of the certificate.
7. Click **Import**.

To follow active connections in semi-real time

1. On the web interface of SPS, 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.



UTC 2018-04-13 13:53:15

File size: 1.7 kB

C:/Users/istva/AppData/Local/One Identity/Safeguard Desktop Player/cache/zat-cache/wJFzef.zat

ENCODE UTF-8

FONT SIZE 12

SESSION ID: svc/tKt7FtUmG8x6nFAmhjN8tr/scbfirst:0

USER: REMOTE USERNAME: zsoltistvanvarga
GATEWAY USERNAME:

CONNECTIONS: CLIENT: 10.30.255.25 PORT: 53585
SERVER: 10.30.255.62 PORT: 22
SOURCE: 10.30.255.25 TARGET: 10.30.255.75

CHANNELS: Session Shell:1

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:

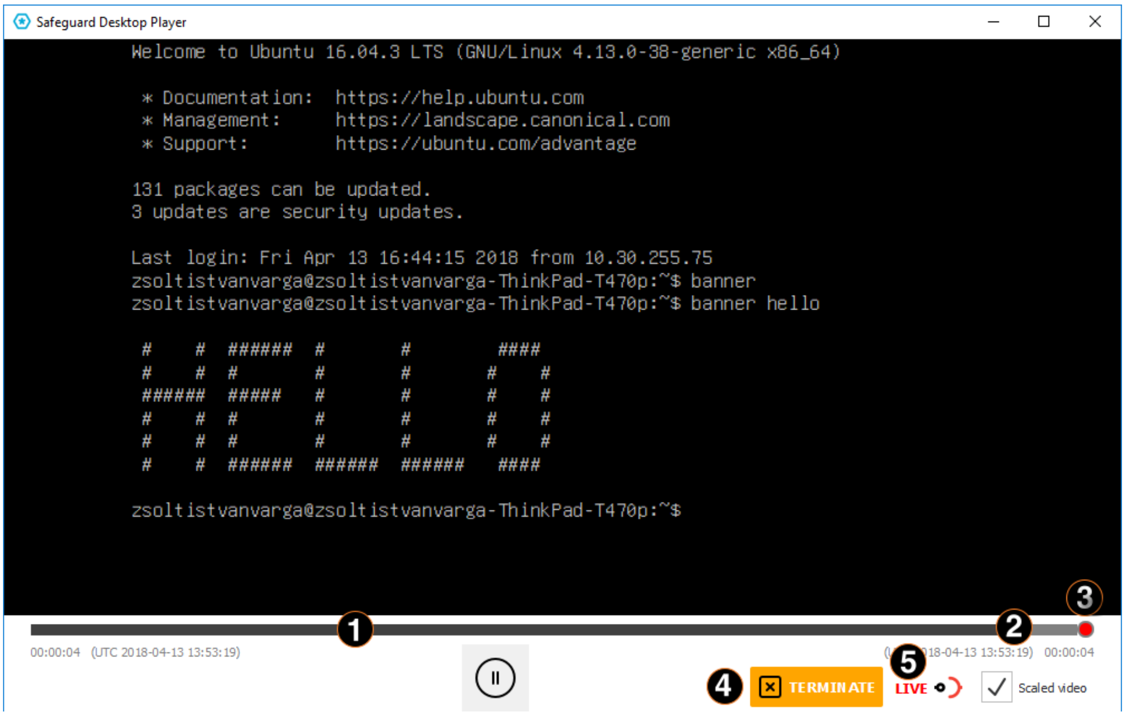
   - LIVE When it is completely red, it indicates that the connection is active and there is some user interaction on the client.

- ᴸᴵⱽᴱ•) 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.

c. **File size.**

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

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 opens.


Safeguard Desktop Player
1
2
3
00:00:04 (UTC 2018-04-13 13:53:19)
(UTC 2018-04-13 13:53:19) 00:00:04
4
☒ TERMINATE
5
LIVE
✓ Scaled video

```
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.13.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

131 packages can be updated.
3 updates are security updates.

Last login: Fri Apr 13 16:44:15 2018 from 10.30.255.75
zsoltistvanvarga@zsoltistvanvarga-ThinkPad-T470p:~$ banner
zsoltistvanvarga@zsoltistvanvarga-ThinkPad-T470p:~$ banner hello

 #    #  ######  #       #        ####
 #    #  #       #       #       #    #
 ######  #####   #       #       #    #
 #    #  #       #       #       #    #
 #    #  #       #       #       #    #
 #    #  ######  ######  ######   ####

zsoltistvanvarga@zsoltistvanvarga-ThinkPad-T470p:~$
```

a. **Blue progress bar.**

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).

b. **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.

c. **Red light.**

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.

d. **Terminate.**

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

e. **LIVE status indicator.**

The indicator shows three different states:

- LIVE When it is completely red, it indicates that the connection is active and there is some user interaction on the client.
- LIVE 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.
- LIVE 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 CONNECTION ENDED 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.

Search 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.

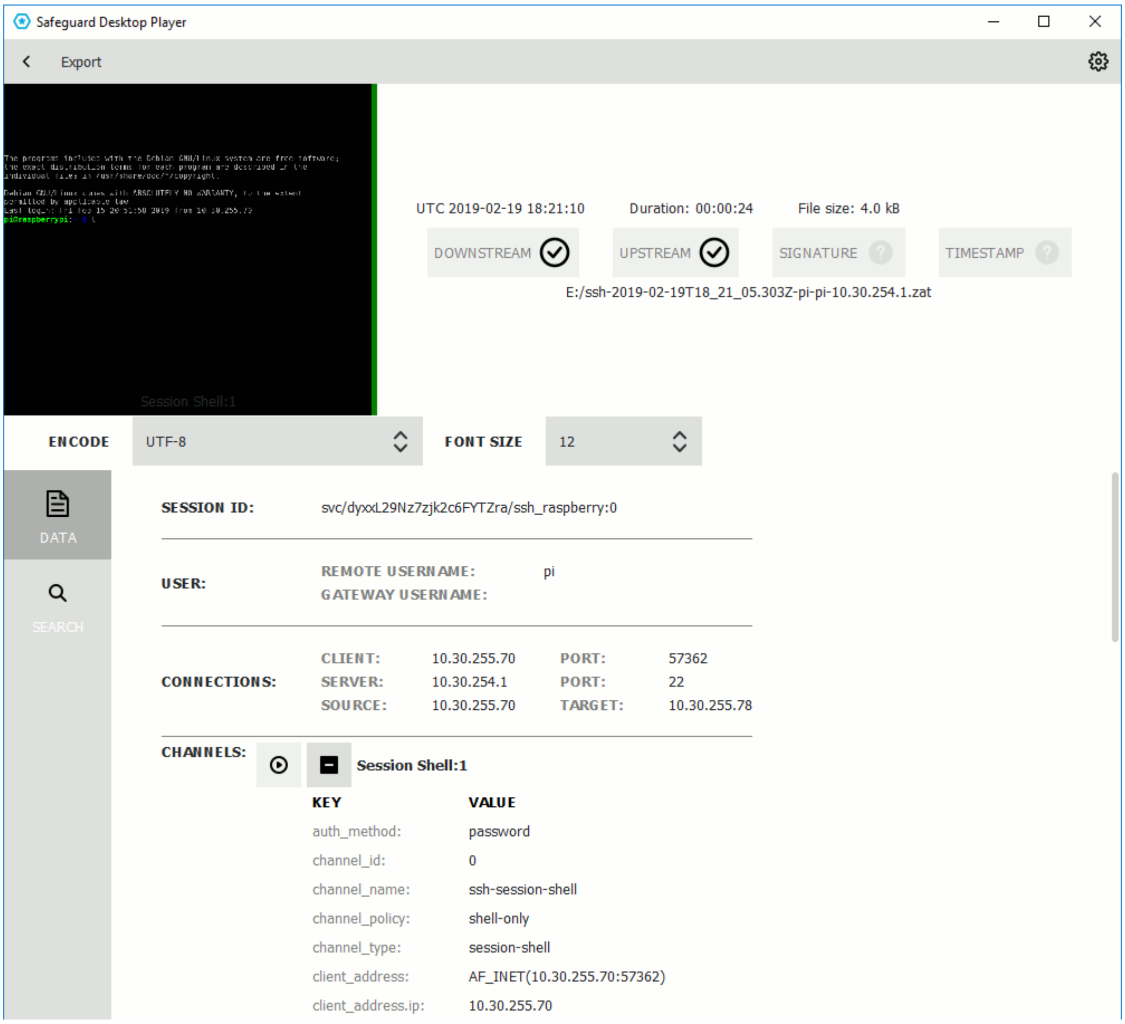
Prerequisites:

- 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 Replay encrypted audit trails.

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



```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Feb 15 20:51:50 2019 from 10.30.255.70
pi@raspberrypi:~ $ l
```

UTC 2019-02-19 18:21:10 Duration: 00:00:24 File size: 4.0 kB

E:/ssh-2019-02-19T18_21_05.303Z-pi-pi-10.30.254.1.zat

ENCODE: UTF-8 FONT SIZE: 12

SESSION ID: svc/dyxxL29Nz7zjk2c6FYTZra/ssh_raspberry:0

USER:
REMOTE USERNAME: pi
GATEWAY USERNAME:

CONNECTIONS:
CLIENT: 10.30.255.70 PORT: 57362
SERVER: 10.30.254.1 PORT: 22
SOURCE: 10.30.255.70 TARGET: 10.30.255.78

CHANNELS: Session Shell:1

KEY	VALUE
auth_method:	password
channel_id:	0
channel_name:	ssh-session-shell
channel_policy:	shell-only
channel_type:	session-shell
client_address:	AF_INET(10.30.255.70:57362)
client_address.ip:	10.30.255.70

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

Search query examples

The following sections provide examples for different search queries.

- For examples of exact matches, see Searching for exact matches on page 34.
- For examples of using boolean operators to combine search keywords, see Combining search keywords on page 35.
- For examples of wildcard searches, see Using wildcard searches on page 36.
- For examples of searching with special characters, see Searching for special characters on page 38.
- For examples of fuzzy search that finds words with similar spelling, see Searching for fuzzy matches on page 40.
- For examples of proximity search to find words that appear within a special distance, see Proximity search on page 40.
- For examples of adjusting the relevance of a search term, see Adjusting the relevance of search terms on page 40.

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 38. 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 an exact phrase, enclose the search keywords in double quotes.

Search expression	`"example command"`
Matches	example command
Does not match	example command example: command

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 keyword2" NOT "keyword2 keyword3"`
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 filters 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 keyword2"^5 "keyword3 keyword4"`
Matches	(returns hits that contain keyword1 keyword2 and keyword3 keyword4, but keyword1 keyword2 is 5-times more relevant)

Export the audit trail as video

The following describes how to export an audit trail as a video file (optionally including the accompanying subtitles). Note that you must open the audit trail in order to export it.

Prerequisites:

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. Note that for Internet Explorer, you must install an add-on.

To export an audit trail as a video file

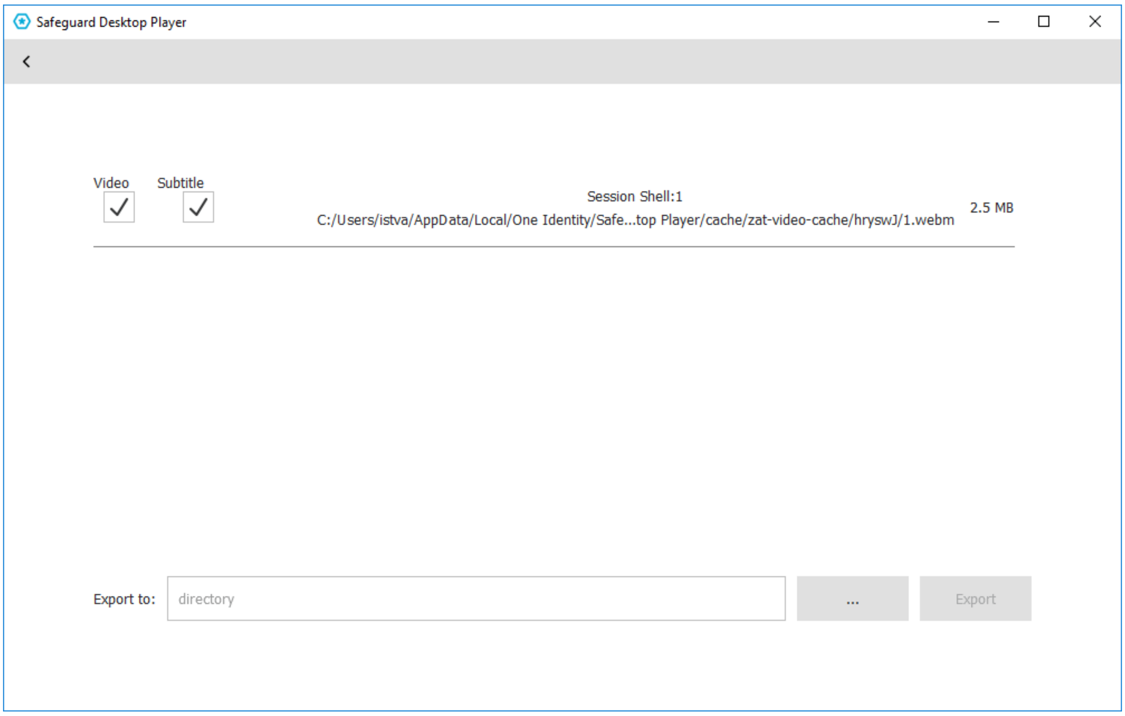
1. Open the audit trail in the Safeguard Desktop Player application.

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



Video ☑ Subtitle ☑

Session Shell:1
C:/Users/istva/AppData/Local/One Identity/Safe...top Player/cache/zat-video-cache/hryswJ/1.webm 2.5 MB

Export to: directory

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

Sharing an encrypted audit trail

The following describes how to share an encrypted audit trail with a third party. 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).

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

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:

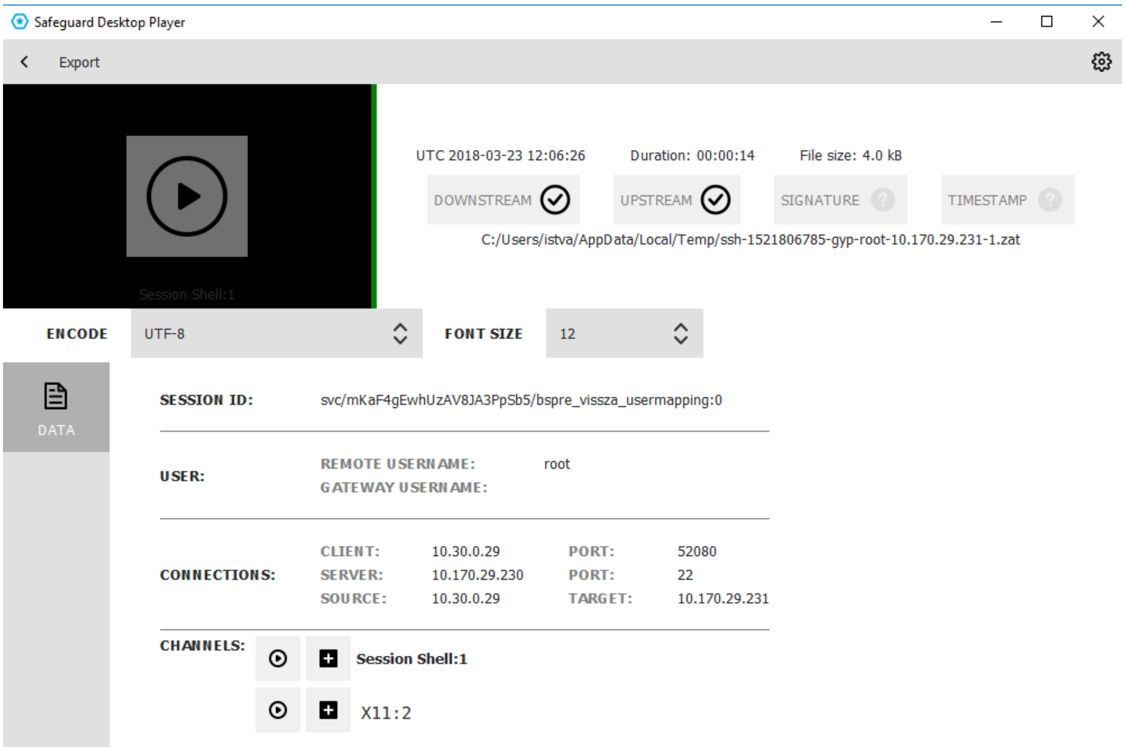
```
./adp --task rekey --file /tmp/ssh-171128T1353-frobert-frobert-
10.30.255.68.zat --key /tmp/indexer-certificate-key.pem: --out /tmp/shared-
ssh.zat --new-cert /tmp/new-encryption-certificate.pem
```

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.

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.



UTC 2018-03-23 12:06:26 Duration: 00:00:14 File size: 4.0 kB

C:/Users/istva/AppData/Local/Temp/ssh-1521806785-gyp-root-10.170.29.231-1.zat

ENCODE UTF-8

FONT SIZE 12

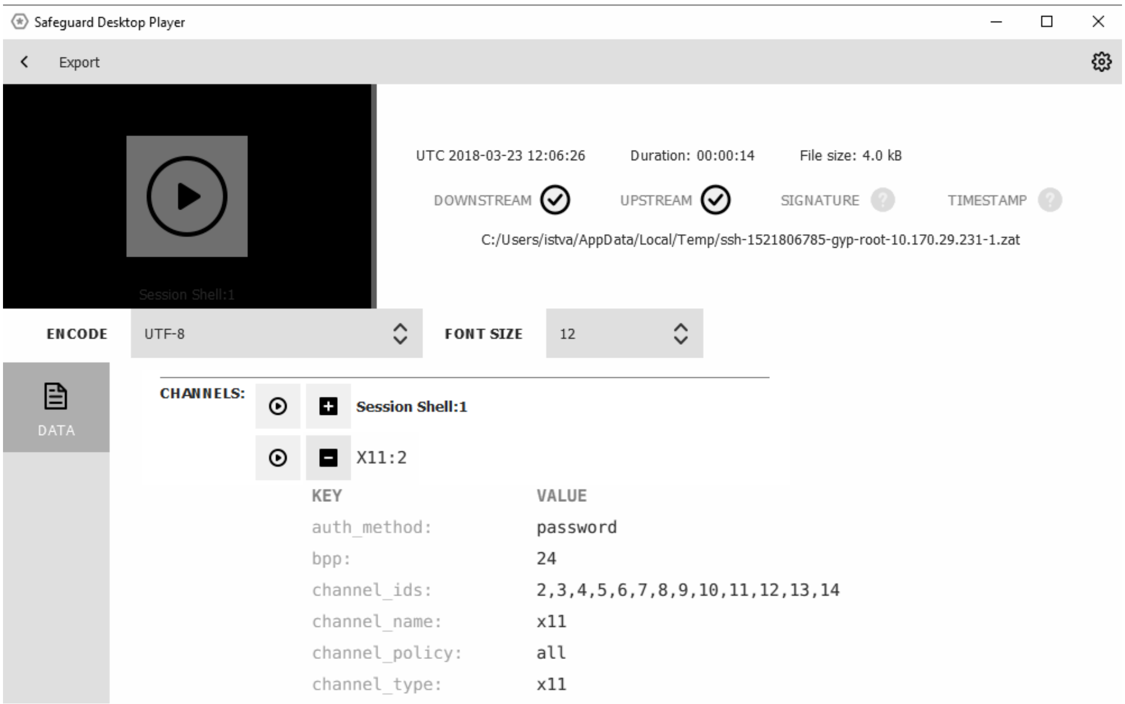
SESSION ID: svc/mKaF4gEwhUzAV8JA3PpSb5/bspre_vissza_usermapping:0

USER: REMOTE USERNAME: root
GATEWAY USERNAME:

CONNECTIONS:
CLIENT: 10.30.0.29 PORT: 52080
SERVER: 10.170.29.230 PORT: 22
SOURCE: 10.30.0.29 TARGET: 10.170.29.231

CHANNELS:
Session Shell:1
X11:2

- 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.



UTC 2018-03-23 12:06:26 Duration: 00:00:14 File size: 4.0 kB

DOWNSTREAM ✓ UPSTREAM ✓ SIGNATURE ? TIMESTAMP ?

C:/Users/istva/AppData/Local/Temp/ssh-1521806785-gyp-root-10.170.29.231-1.zat

ENCODE UTF-8 FONT SIZE 12

CHANNELS:
- Session Shell:1
- X11:2

KEY	VALUE
auth_method:	password
bpp:	24
channel_ids:	2,3,4,5,6,7,8,9,10,11,12,13,14
channel_name:	x11
channel_policy:	all
channel_type:	x11

- The Safeguard Desktop Player stores the fonts used to display the texts in the audit trail in the `<desktop-player-installation-folder>/fonts` folder.

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

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

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

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, `~/SafeguardDesktopPlayer` on Linux, and `/Applications/Safeguard Desktop Player.app/Contents/Resources/` on MacOS.

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

   Linux or *MacOS*: **./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.

15

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

The following 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, it is `C:\Documents and Settings\<username>\Software\Safeguard\Safeguard Desktop Player\` on Microsoft Windows platforms, `~/SafeguardDesktopPlayer` on Linux, and `/Applications/Safeguard Desktop Player.app/Contents/Resources/` on MacOS.

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 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 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 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.

Export raw network traffic in PCAP format using the GUI

The following 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 Replay encrypted audit trails.

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.

16

Export screen content text

The following describes how to export screen content text from text-based protocols (that is, 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 (that is, 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 Replay encrypted audit trails.

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

17

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**

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 Replay 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 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`, `.zatx`, 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 Force software rendering.

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**

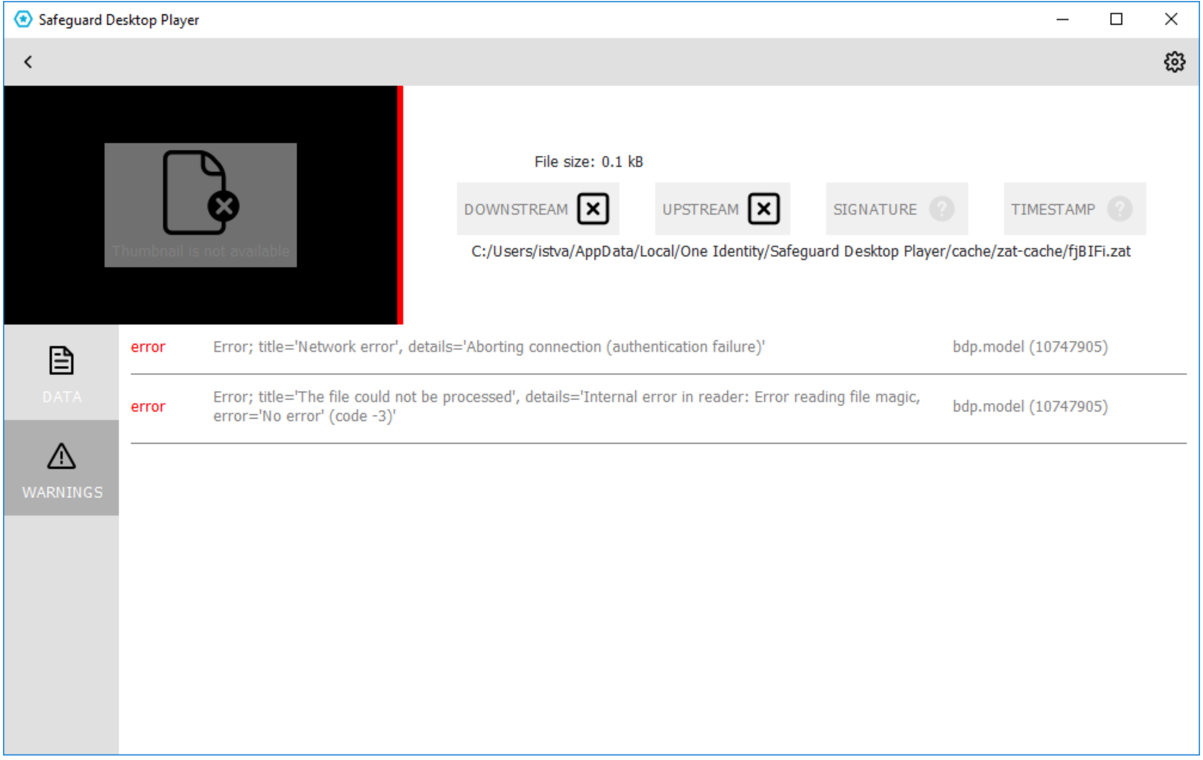
Cannot import CA certificate

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



File size: 0.1 kB

C:/Users/istva/AppData/Local/One Identity/Safeguard Desktop Player/cache/zat-cache/fjBIFi.zat

```
error    Error; title='Network error', details='Aborting connection (authentication failure)'    bdp.model (10747905)
error    Error; title='The file could not be processed', details='Internal error in reader: Error reading file magic,    bdp.model (10747905)
         error='No error' (code -3)'
```

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"**

18

Install Safeguard Desktop Player

To install the Safeguard Desktop Player application, read the following sections.

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.

- **Mac:**

  macOS High Sierra 10.13, or newer.

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

The following describes how to install the Safeguard Desktop Player 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.

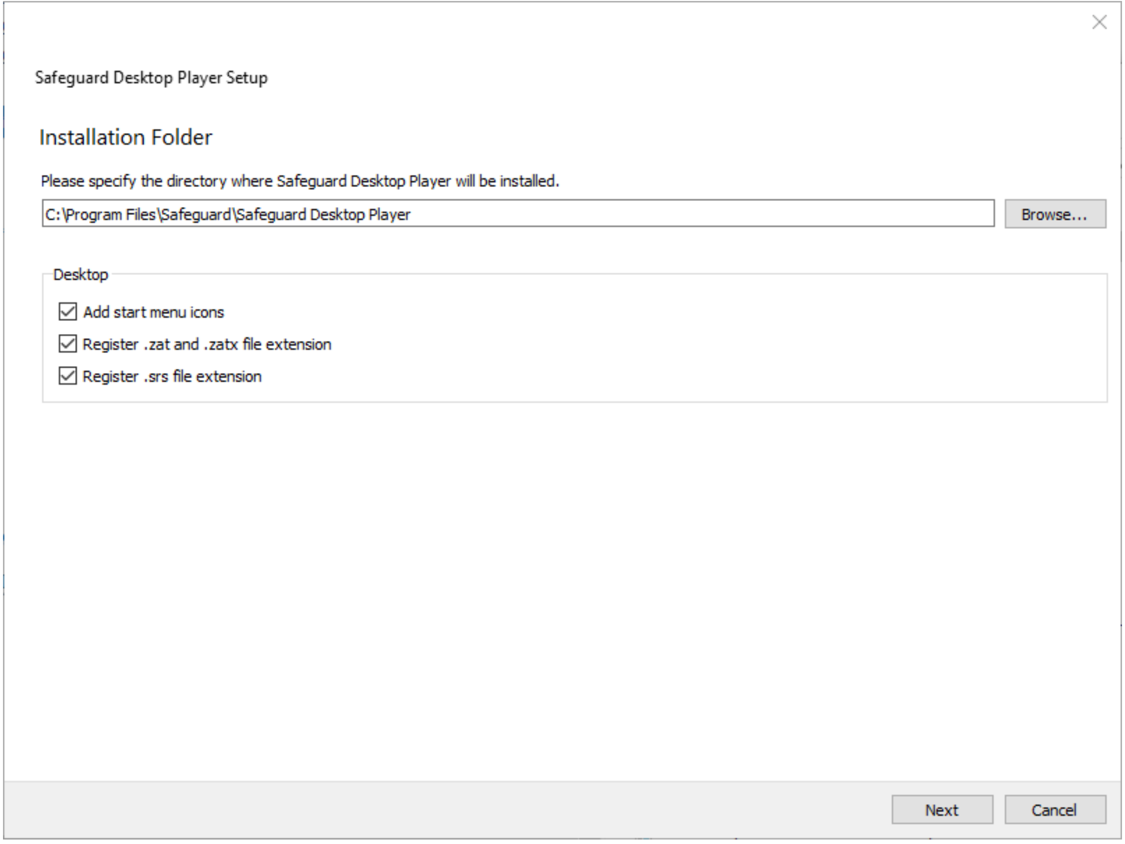
  For details, see Safeguard Desktop Player system requirements.
- If you already have an earlier version of the Safeguard Desktop Player application installed on the host, uninstall the previous installation. If you want to keep the previous installation for some reason, install the new version into a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

To install the Safeguard Desktop Player application

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**.

Figure 2: Select the installation folder



Safeguard Desktop Player Setup

Installation Folder

Please specify the directory where Safeguard Desktop Player will be installed.

C:\Program Files\Safeguard\Safeguard Desktop Player

Desktop

☑ Add start menu icons

☑ Register .zat and .zatx file extension

☑ Register .srs file extension

3. 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**.

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

Install Safeguard Desktop Player on Linux

The following 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 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 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 into 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 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:

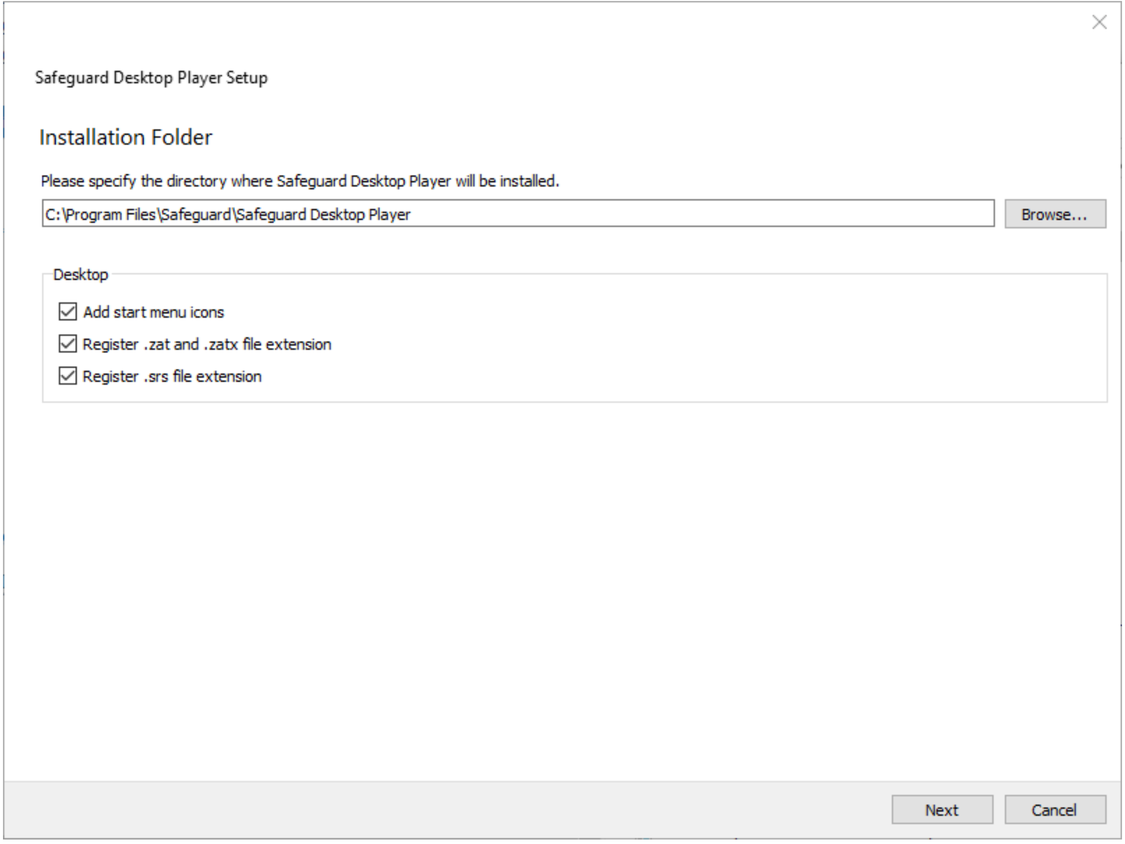
     ```
     chmod +x ./desktop_player_installer.1.0.17.release.run; sudo ./desktop_
     player_installer.1.0.17.release.run
     ```

   - *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**.

Figure 3: Select the installation folder



Safeguard Desktop Player Setup

Installation Folder

Please specify the directory where Safeguard Desktop Player will be installed.

C:\Program Files\Safeguard\Safeguard Desktop Player

Desktop

☑ Add start menu icons

☑ Register .zat and .zatx file extension

☑ Register .srs file extension

4. 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**.

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

Install Safeguard Desktop Player on Mac

The following describes how to install the Safeguard Desktop Player application.

Prerequisites:

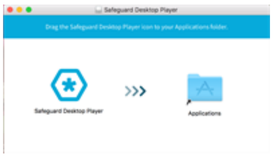
- You must have a valid support portal account with access to SPS downloads.
- macOS High Sierra 10.13, or newer.

  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 into 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 app to the Applications folder.

   Figure 4: Drag app to the Applications folder

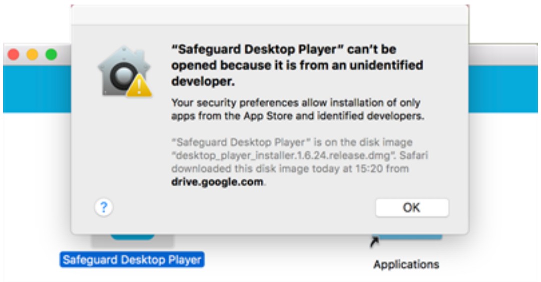
   

   Safeguard Desktop Player

   Drag the Safeguard Desktop Player icon to your Applications folder.

3. If your Mac is set to allow apps 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

   "Safeguard Desktop Player" can't be opened because it is from an unidentified developer.

   Your security preferences allow installation of only apps from the App Store and identified developers.

   "Safeguard Desktop Player" is on the disk image "desktop_player_installer.1.6.24.release.dmg". Safari downloaded this disk image today at 15:20 from **drive.google.com**.

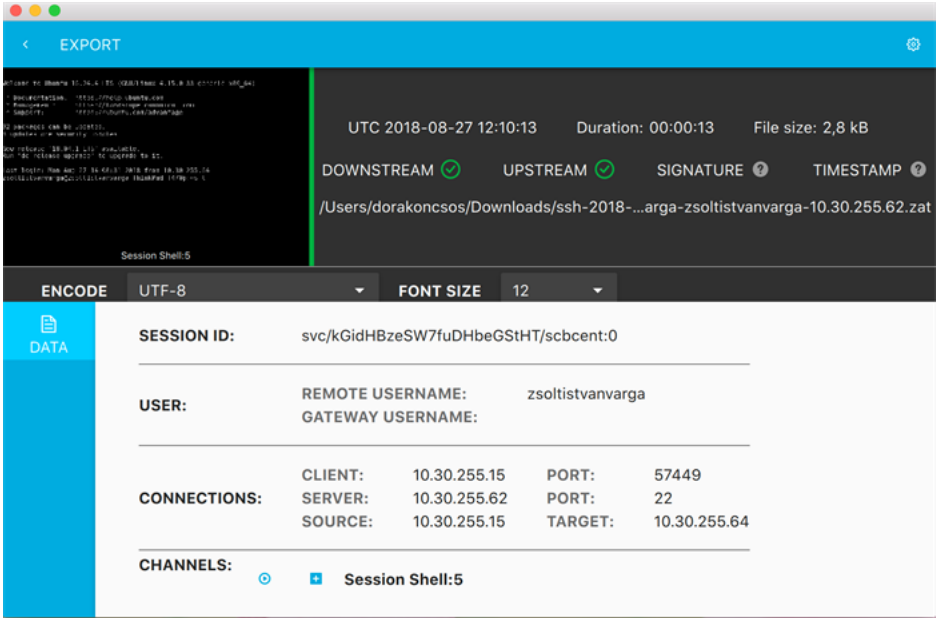
   a. In **Finder**, control-click the Safeguard Desktop Player application.

   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 in the future by double-clicking it, just as you can any authorized app.

4. Open an audit trail to replay. For more information, see Replay audit trails.

Figure 6: Replay audit trail



UTC 2018-08-27 12:10:13 Duration: 00:00:13 File size: 2,8 kB

DOWNSTREAM ✓ UPSTREAM ✓ SIGNATURE ? TIMESTAMP ?

/Users/dorakoncsos/Downloads/ssh-2018-...arga-zsoltistvanvarga-10.30.255.62.zat

ENCODE: UTF-8
FONT SIZE: 12

SESSION ID: svc/kGidHBzeSW7fuDHbeGStHT/scbcent:0

USER:
REMOTE USERNAME: zsoltistvanvarga
GATEWAY USERNAME:

CONNECTIONS:
CLIENT: 10.30.255.15 PORT: 57449
SERVER: 10.30.255.62 PORT: 22
SOURCE: 10.30.255.15 TARGET: 10.30.255.64

CHANNELS: Session Shell:5

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`
- 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 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