One Identity Safeguard for Privileged Sessions 5.7

Upgrade Guide

Legend

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

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

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

SPS Upgrade Guide
Updated - July 2018
Version - 5.7

Contents

Preface

Welcome to One Identity Safeguard for Privileged Sessions (Safeguard for Privileged Sessions) version 5 F7 and thank you for choosing our product. This document describes the upgrade process from existing Safeguard for Privileged Sessions installations to Safeguard for Privileged Sessions 5 F7. The main goal of this paper is to help system administrators in planning the migration to the new version of Safeguard for Privileged Sessions.

CAUTION:

Read the entire document thoroughly before starting the upgrade.

This document covers the One Identity Safeguard for Privileged Sessions 5 F7 product.

Versions and releases of Safeguard for Privileged Sessions

As of June 2011, the following release policy applies to One Identity Safeguard for Privileged Sessions:

- *Long Term Supported or LTS releases* (for example, Safeguard for Privileged Sessions 4 LTS) are supported for 3 years after their original publication date and for 1 year after the next LTS release is published (whichever date is later). The second digit of the revisions of such releases is 0 (for example, Safeguard for Privileged Sessions 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, Safeguard for Privileged Sessions 4 F1) are supported for 6 months after their original publication date and for 2 months after a succeeding Feature or LTS release is published (whichever date is later). Feature releases contain enhancements and new features, presumably 1-3 new features per release. Only the last feature release is supported (for example, when a new feature release comes out, the last one becomes unsupported in 2 months).

For a full description of stable and feature releases, open the SPS product page on the Support Portal and navigate to **Product Life Cycle & Policies > Product Support Policies > Software Product Support Lifecycle Policy**.

CAUTION:

Downgrading from a feature release is not supported. If you upgrade from an LTS release (for example, 4.0) to a feature release (4.1), you have to keep upgrading with each new feature release until the next LTS version (in this case, 5.0) is published.

Prerequisites for upgrading Safeguard for Privileged Sessions

This section describes the requirements and steps to perform before starting the Safeguard for Privileged Sessions upgrade process.

- You must have a valid software subscription to be able to download the new version of Safeguard for Privileged Sessions, and also the new license file.
- You will need a support portal account to download the required ISO image. Note that the registration is not automatic, and might take up to two working days to be processed.
- Back up your configuration and your data.

  For more information on creating configuration and data backups, see "Data and configuration backups" in the Administration Guide.
- Export your configuration.

  For more information, see "Exporting the configuration of Safeguard for Privileged Sessions" in the Administration Guide.
- Verify that Safeguard for Privileged Sessions is in good condition (no issues are displayed on the System Monitor).
- Optional: If you have core dump files that are necessary for debugging, download them from **Basic Settings > Troubleshooting > Core files**. These files are removed during the upgrade process.

If you have a high availability cluster:

- Verify that you have IPMI access to the slave node. You can find detailed information on using the IPMI interface in the following documents:

  For Safeguard for Privileged Sessions T4 and T10, see the X9 SMT IPMI User's Guide. For Safeguard for Privileged Sessions T1, see the SMT IPMI User's Guide.
- On the **Basic Settings > High Availability** page, verify that the HA status is not degraded.

If you are upgrading Safeguard for Privileged Sessions in a virtual environment:

- Create a snapshot of the virtual machine before starting the upgrade process.
- Configure and enable console redirection (if the virtual environment allows it).

Notes and warnings about the upgrade

The following is a list of important notes and warnings about the upgrade process and changes in Safeguard for Privileged Sessions 5 F7.

CAUTION:

As part of the upgrade, Safeguard for Privileged Sessions upgrades its session database. Depending on the size of the session database, this process can take several days to finish. You can check the status of the upgrade process in the System Monitor.

During this upgrade, the session database used when searching on the REST API and the new Search interface is incomplete, and older sessions might not appear in the search results. The classic search is unaffected.

If there are any errors during the upgrade, contact our Support Team.

CAUTION:

Safeguard for Privileged Sessions 5 F4 and later versions use a new encryption algorithm to encrypt the recorded audit trails (AES128-GCM). This change has the following effects:

- **If you are using external indexers to index your audit trails, you must upgrade them to the latest version. Earlier versions will not be able to index encrypted audit trails recorded with Safeguard for Privileged Sessions 5 F4 and later.**
- **To replay an encrypted audit trail recorded with Safeguard for Privileged Sessions 5 F4 or later, you can use the latest version of the Safeguard Desktop Player application, or the browser-based player of Safeguard for Privileged Sessions. You cannot replay such audit trails using earlier versions of Safeguard Desktop Player, nor any version of the Audit Player application.**

CAUTION:

It is no longer possible to search for screen contents indexed by the old Audit Player on the new search UI and the REST interface. Searching in session metadata (such as IP addresses and usernames) and in extracted events (such as executed commands and window titles that appeared on the screen) remains possible.

As the old Audit Player was replaced and deprecated as an indexing tool during the 4.x versions, this should only affect very old sessions. Sessions that were processed by the new indexing service will work perfectly. If you wish to do screen content searches in historical sessions, contact our Support Team.

Upgrading from Safeguard for Privileged Sessions 5.0.0 or later:

CAUTION:

Physical Safeguard for Privileged Sessions appliances based on Pyramid hardware are not supported in 5 F1 and later feature releases. Do not upgrade to 5 F1 or later on a Pyramid-based hardware. The last supported release for this hardware is 5 LTS, which is a long-term supported release.

If you have purchased Safeguard for Privileged Sessions before August, 2014 and have not received a replacement hardware since then, you have Pyramid hardware, so do not upgrade to Safeguard for Privileged Sessions 5 F1 or later. If you have purchased Safeguard for Privileged Sessions after August 2014, you can upgrade to 5 F1.

If you do not know the type of your hardware or when it was purchased, complete the following steps:

1. **Login to Safeguard for Privileged Sessions.**
2. **Navigate to Basic Settings > Troubleshooting > Create debug bundle for support ticket, click Create and save debug bundle from current system state, and save the file.**
3. **Open a ticket at https://support.oneidentity.com/create-service-request/.**
4. **Upload the file you downloaded from Safeguard for Privileged Sessions in Step 1.**
5. **We will check the type of your hardware and notify you.**

Upgrade path to Safeguard for Privileged Sessions 5 F7

Upgrading to Safeguard for Privileged Sessions 5 F7 is tested and supported using the following upgrade path:

- *The latest Safeguard for Privileged Sessions 5 LTS maintenance version (for example, 5.0.x) -> Safeguard for Privileged Sessions 5 F7*

  Always upgrade to the latest available maintenance version of Safeguard for Privileged Sessions 5 LTS before upgrading to Safeguard for Privileged Sessions 5 F7.
- *The latest maintenance versions of the previous three feature releases (in this case, Safeguard for Privileged Sessions 5 F3 or later) -> Safeguard for Privileged Sessions 5 F7*

  Always upgrade to the latest available maintenance version of the feature release before upgrading to Safeguard for Privileged Sessions 5 F7.

From older releases, upgrade to 5 LTS first. For details, see How to upgrade to One Identity Safeguard for Privileged Sessions 5 LTS.

Upgrading to Safeguard for Privileged Sessions 5 F7

Purpose:

If you want to upgrade a Safeguard for Privileged Sessions cluster, see . To upgrade a standalone Safeguard for Privileged Sessions node to version 5 F7, complete the following steps.

Prerequisites:

Read the following warnings before starting the upgrade process.

CAUTION:

- **After performing the upgrade, it is not possible to downgrade to the earlier version. Upgrading to Safeguard for Privileged Sessions 5 F7 is an irreversible process.**
- **It is recommended to test the upgrade process first in VMware. To do this, download a VMware image of the latest Safeguard for Privileged Sessions version, import the configuration of your Safeguard for Privileged Sessions into this VMware version, and perform the upgrade. If everything is working, perform the upgrade on the production system.**

Steps:

Complete the prerequisites described in and upgrade Safeguard for Privileged Sessions to the latest revision of the current version.

Login to your support portal.

Download the Safeguard for Privileged Sessions 5 F7 firmware filesfrom the Downloads page.

Upload the latest 5 F7 firmware filesto your Safeguard for Privileged Sessions. For details, see Upgrading Safeguard for Privileged Sessions in *The One Identity Safeguard for Privileged Sessions 5 LTS Administrator Guide*.

Click **Test** for the new firmware to check if your configuration can be upgraded to version 5

F7. If the test returns any errors, correct them before continuing the upgrade process. If you encounter any problems, contact our Support Team.

Select **After reboot**.

CAUTION:

Proceed only if the upgrade test is successful.

Activate the firmware.

Recommended step. To help troubleshoot potential issues following the upgrade, collect and save system information (create a debug bundle) now.

Navigate to **Basic Settings > Troubleshooting > Create debug bundle for support ticket** and choose **Create and save debug bundle from current system state**.

CAUTION:

Do NOT click Reboot cluster during the upgrade process unless explicitly instructed.

Navigate to **Basic Settings > System > System Control > This node > Reboot** to reboot the machine. Safeguard for Privileged Sessions will start with the new firmware and upgrade its configuration, database, and other system components. During the upgrade process, Safeguard for Privileged Sessions displays status information and other data on the local console and on the web interface of Safeguard for Privileged Sessions, at any of the **Listening addresses** configured at **Basic settings > Local Services > Web login (admin and user)**.

NOTE:

If you are upgrading to version 5 F7 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 5 F7. So during the upgrade to version 5 F7, you will not be able to see any upgrade logs on the web interface.

CAUTION:

If the connection database is large and contains information about several thousands of sessions, the upgrade process can take about 15-20 minutes or more, depending on the actual hardware.

CAUTION:

After the reboot in 5 F7, Safeguard for Privileged Sessions will start importing large amounts of data from metadb. This process can take about 30-40 minutes or more. During the import process, the REST base search might not function properly, since the data to search in might still be incomplete.

To make sure that the import process has finished, check the logs.

Navigate to Basic Settings > Troubleshooting > View log files. Select `syslog` **as Logtype, the day of the upgrade process as Day and enter** `Run metadb_importer.py` **in the Show only messages containing field. Click View.**

If the import process has finished, the following line is displayed:

```
systemd[1]: Started Run metadb_importer.py to import data from metadb to elast-
icsearch if necessary...
```

CAUTION:

In case the Safeguard for Privileged Sessions web interface is not available within 30 minutes of rebooting Safeguard for Privileged Sessions, check the information displayed on the local console and contact our Support Team.

If you experience any strange behavior of the web interface, first try to reload the page by holding the SHIFT key while clicking the Reload button of your browser to remove any cached version of the page.

NOTE:

In the unlikely case that Safeguard for Privileged Sessions encounters a problem during the upgrade process and cannot revert to its original state, Safeguard for Privileged Sessions performs the following actions:

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH-access to Safeguard for Privileged Sessions, unless Safeguard for Privileged Sessions is running in sealed mode. That way it is possible to access the logs of the upgrade process, which helps the One Identity Support Team to diagnose and solve the problem. Note that SSH access will be enabled on every active interface, even if management access has not been enabled for the interface.

Navigate to **Basic Settings > System > Version details** and verify that Safeguard for Privileged Sessions is running version 5 F7 of the firmware. If not, it means that the upgrade process did not complete properly and Safeguard for Privileged Sessions performed a rollback to revert to the earlier firmware version. In this case, complete the following steps:

1. Navigate to **Basic Settings > Troubleshooting > Create debug bundle for support ticket** and click **Create and save debug bundle from current system state**.
2. Save the resulting ZIP file.
3. Contact the One Identity Support Team and send them the file. They will analyze its contents to determine why the upgrade was not completed and assist you in solving the problem.

Upgrade your Safeguard Desktop Player installations to the latest version. For details, see Upgrading the Safeguard Desktop Player.

CAUTION:

As part of the upgrade, Safeguard for Privileged Sessions upgrades its session database. Depending on the size of the session database, this process can take several days to finish. You can check the status of the upgrade process in the System Monitor.

1. **During this upgrade, the session database used when searching on**

the REST API and the new Search interface is incomplete, and older sessions might not appear in the search results. The classic search is unaffected.

If there are any errors during the upgrade, contact our Support Team.

2. *Optional step:* If Safeguard for Privileged Sessions was in a domain before the upgrade, navigate to **RDP Control -> Domain membership** and make sure that your domain-related settings are correct. In case of correct settings, you will see the following:
   - **Fully qualified domain name (realm name): Host joined currently configured domain successfully.**
   - **Currently joined domains:** `<name.of.the.joined.domain>`

   This is important becacuse in rare cases, the appliance might fall out from the domain after an upgrade, and a manual rejoin might be required based on its status.

Upgrading the Safeguard Desktop Player

Upgrading the Safeguard Desktop Player application is only a simple installation process. See the Safeguard Desktop Player User Guide for details. You can download the Safeguard Desktop Player application from the Downloads page.

CAUTION:

Safeguard for Privileged Sessions 5 F4 and later versions use a new encryption algorithm to encrypt the recorded audit trails (AES128-GCM). This change has the following effects:

- **If you are using external indexers to index your audit trails, you must upgrade them to the latest version. Earlier versions will not be able to index encrypted audit trails recorded with Safeguard for Privileged Sessions 5 F4 and later.**
- **To replay an encrypted audit trail recorded with Safeguard for Privileged Sessions 5 F4 or later, you can use the latest version of the Safeguard Desktop Player application, or the browser-based player of Safeguard for Privileged Sessions. You cannot replay such audit trails using earlier versions of Safeguard Desktop Player, nor any version of the Audit Player application.**

Upgrading the external indexer

To upgrade the indexer application on your external indexer hosts, complete the following steps.

CAUTION:

Safeguard for Privileged Sessions 5 F4 and later versions use a new encryption algorithm to encrypt the recorded audit trails (AES128-GCM). This change has the following effects:

- **If you are using external indexers to index your audit trails, you must upgrade them to the latest version. Earlier versions will not be able to index encrypted audit trails recorded with Safeguard for Privileged Sessions 5 F4 and later.**
- **To replay an encrypted audit trail recorded with Safeguard for Privileged Sessions 5 F4 or later, you can use the latest version of the Safeguard Desktop Player application, or the browser-based player of Safeguard for Privileged Sessions. You cannot replay such audit trails using earlier versions of Safeguard Desktop Player, nor any version of the Audit Player application.**

Prerequisites:

Before you start, create a backup copy of the `/opt/external-indexer/etc/indexer/indexerworker.cfg` and `/opt/external-indexer/etc/indexer/indexer-certs.cfg` indexer configuration files.

Steps:

1. Download the latest indexer package from the Downloads page.
2. Copy the downloaded `.rpm` package to your external indexer hosts.
3. Stop the indexer by using the following command.
   - On Red Hat or CentOS 6.5:

     ```
     service external-indexer stop
     ```

- On Red Hat or CentOS 7:

  ```
  systemctl stop external-indexer.service
  ```

4. Execute the following command: **yum upgrade -y indexer.rpm**
5. Resolve any warnings displayed during the upgrade process.
6. Restart the indexer by using the following command.
   - On Red Hat or CentOS 6.5:

     ```
     service external-indexer start
     ```

   - On Red Hat or CentOS 7:

     ```
     systemctl start external-indexer.service
     ```

7. Repeat this procedure on every indexer host.

Upgrading a Safeguard for Privileged Sessions cluster to 5 F7

Prerequisites:

Make sure that you have physically connected the IPMI interface to the network and that it is properly configured. This is important because you can only power the slave node on through the IPMI interface. For details on configuring the IPMI interface, see "Out-of-band management of Safeguard for Privileged Sessions" in the Administration Guide.

Purpose:

To upgrade a Safeguard for Privileged Sessions high-availability cluster, complete the following steps.

CAUTION:

- **After performing the upgrade, it is not possible to downgrade to the earlier version. Upgrading to Safeguard for Privileged Sessions 5 F7 is an irreversible process.**
- **It is recommended to test the upgrade process first in VMware. To do this, download a VMware image of the latest Safeguard for Privileged Sessions version, import the configuration of your Safeguard for Privileged Sessions into this VMware version, and perform the upgrade. If everything is working, perform the upgrade on the production system.**

CAUTION:

Do NOT reboot any of the Safeguard for Privileged Sessions nodes unless explicitly instructed.

CAUTION:

Do NOT click Reboot cluster during the upgrade process unless explicitly instructed.

Steps:

Complete the prerequisites described in and upgrade Safeguard for Privileged Sessions to the latest revision of the current version.

Login to your support portal.

Download the Safeguard for Privileged Sessions 5 F7 firmware filesfrom the Downloads page.

Upload the latest 5 F7 firmware filesto your Safeguard for Privileged Sessions. For details, see Upgrading Safeguard for Privileged Sessions in *The One Identity Safeguard for Privileged Sessions 5 LTS Administrator Guide*.

Click **Test** for the new firmware to check if your configuration can be upgraded to version 5 F7. If the test returns any errors, correct them before continuing the upgrade process. If you encounter any problems, contact our Support Team.

Select **After reboot**.

CAUTION:

Proceed only if the upgrade test is successful.

Activate the firmware.

Recommended step. To help troubleshoot potential issues following the upgrade, collect and save system information (create a debug bundle) now.

Navigate to **Basic Settings > Troubleshooting > Create debug bundle for support ticket** and choose **Create and save debug bundle from current system state**.

CAUTION:

Do NOT click Reboot cluster during the upgrade process unless explicitly instructed.

Navigate to **Basic Settings > System > System Control > This node > Reboot** to reboot the machine. Safeguard for Privileged Sessions will start with the new firmware and upgrade its configuration, database, and other system components. During the upgrade process, Safeguard for Privileged Sessions displays status information and other data on the local console and on the web interface of Safeguard for Privileged Sessions, at any of the **Listening addresses** configured at **Basic settings > Local Services > Web login (admin and user)**.

NOTE:

If you are upgrading to version 5 F7 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 5 F7. So during the upgrade to version 5 F7, you will not be able to see any upgrade logs on the web interface.

CAUTION:

If the connection database is large and contains information about several thousands of sessions, the upgrade process can take about 15-20 minutes or more, depending on the actual hardware.

CAUTION:

After the reboot in 5 F7, Safeguard for Privileged Sessions will start importing large amounts of data from metadb. This process can take about 30-40 minutes or more. During the import process, the REST base search might not function properly, since the data to search in might still be incomplete.

To make sure that the import process has finished, check the logs.

Navigate to Basic Settings > Troubleshooting > View log files. Select `syslog` **as Logtype, the day of the upgrade process as Day and enter** `Run metadb_importer.py` **in the Show only messages containing field. Click View.**

If the import process has finished, the following line is displayed:

```
systemd[1]: Started Run metadb_importer.py to import data from metadb to elast-
icsearch if necessary...
```

CAUTION:

In case the Safeguard for Privileged Sessions web interface is not available within 30 minutes of rebooting Safeguard for Privileged Sessions, check the information displayed on the local console and contact our Support Team.

If you experience any strange behavior of the web interface, first try to reload the page by holding the SHIFT key while clicking the Reload button of your browser to remove any cached version of the page.

NOTE:

In the unlikely case that Safeguard for Privileged Sessions encounters a problem during the upgrade process and cannot revert to its original state, Safeguard for Privileged Sessions performs the following actions:

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH-access to Safeguard for Privileged Sessions, unless Safeguard for Privileged Sessions is running in sealed mode. That way it is possible to access the logs of the upgrade process, which helps the One Identity Support Team to diagnose and solve the problem. Note that SSH access will be enabled on every active interface, even if management access has not been enabled for the interface.

Navigate to **Basic Settings > System > Version details** and verify that Safeguard for Privileged Sessions is running version 5 F7 of the firmware. If not, it means that the upgrade process did not complete properly and Safeguard for Privileged Sessions performed a rollback to revert to the earlier firmware version. In this case, complete the following steps:

1. Navigate to **Basic Settings > Troubleshooting > Create debug bundle for support ticket** and click **Create and save debug bundle from current system state**.
2. Save the resulting ZIP file.
3. Contact the One Identity Support Team and send them the file. They will analyze its contents to determine why the upgrade was not completed and assist you in solving the problem.

Upgrade your Safeguard Desktop Player installations to the latest version. For details, see Upgrading the Safeguard Desktop Player.

1. Wait until the new firmware is synchronized to the slave node. This is usually completed within 60 seconds.
2. Navigate to **Basic Settings > High availability & Nodes > Other node** and click **Shutdown** to power off the slave node.

   CAUTION:

   Do not power on the slave node.

3. If the master reboot has been successful, power up the slave node through IPMI.

   CAUTION:

   As part of the upgrade, Safeguard for Privileged Sessions upgrades its session database. Depending on the size of the session database, this process can take several days to finish. You can check the status of the upgrade process in the System Monitor.

   During this upgrade, the session database used when searching on the REST API and the new Search interface is incomplete, and older sessions might not appear in the search results. The classic search is unaffected.

   If there are any errors during the upgrade, contact our Support Team.

4.

5. If Safeguard for Privileged Sessions is functioning properly after the upgrade, power up the slave node through the IMPI web interface.

   The slave node attempts to boot with the new firmware, and reconnects to the master node to sync data. During the sync process, certain services (including Heartbeat) are not available. Wait for the process to finish, and the slave node to boot fully.

10

Troubleshooting

If you experience any strange behavior of the web interface, first try to reload the page by holding the SHIFT key while clicking the Reload button of your browser to remove any cached version of the page.

In the unlikely case that Safeguard for Privileged Sessions encounters a problem during the upgrade process and cannot revert to its original state, Safeguard for Privileged Sessions performs the following actions:

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH-access to Safeguard for Privileged Sessions, unless Safeguard for Privileged Sessions is running in sealed mode. That way it is possible to access the logs of the upgrade process that helps the One Identity Support Team to diagnose and solve the problem. Note that SSH access will be enabled on every active interface, even if management access has not been enabled for the interface.

In case the web interface is not available within 30 minutes of rebooting Safeguard for Privileged Sessions, check the information displayed on the local console and contact our Support Team.

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