One Identity Safeguard for Privileged Sessions 6.1

Upgrade Guide

Legend

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

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

SPS Upgrade Guide
Updated - August 2019
Version - 6.1

Contents

Preface **4**
Versions and releases of One Identity Safeguard for Privileged Sessions (SPS) 4
Prerequisites for upgrading SPS **6**
Upgrade path to SPS 6.1 ..... **9**
Upgrading a single SPS node to 6.1 ..... **10**
Upgrading the Safeguard Desktop Player **13**
Upgrading the external indexer **14**
Upgrading an SPS high-availability cluster to 6.1 ..... **15**
Upgrading an SPS central cluster to 6.1 ..... **19**
Troubleshooting **20**
About us **21**
Contacting us 21
Technical support resources 21

1

Preface

Welcome to One Identity Safeguard for Privileged Sessions (SPS) version 6.1 and thank you for choosing our product. This document describes the upgrade process from existing SPS installations to SPS 6.1. The main goal of this paper is to help system administrators in planning the migration to the new version of SPS.

CAUTION:

Read the entire document thoroughly before starting the upgrade.

This document covers the One Identity Safeguard for Privileged Sessions 6.1 product.

Versions and releases of One Identity Safeguard for Privileged Sessions (SPS)

The following release policy applies to One Identity Safeguard for Privileged Sessions (SPS):

- *Long Term Supported or LTS releases* (for example, SPS 6.0) 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, SPS 6.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, SPS 6.1) 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 long-term-supported 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, 6.0) to a feature release (6.1), you have to keep upgrading with each new feature release until the next LTS version (in this case, 7.0) is published.

2

Prerequisites for upgrading SPS

This section describes the requirements and steps to perform before starting the SPS upgrade process.

General requirements:

- You must have a valid software subscription to be able to download the new version of SPS.
- 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 One Identity Safeguard for Privileged Sessions (SPS)" in the Administration Guide.
- Verify that SPS 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 Sessions Appliance 3000 and 3500, see the X9 SMT IPMI User's Guide.
- On the **Basic Settings > High Availability** page, verify that the HA status is not degraded.

If you are upgrading SPS 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).

If you are using a plugin (for example, a Credential Store plugin, or a multi-factor

authentication plugin):

- You will need an updated version of the plugin you are using. Download it from Downloads page.

Notes and warnings about the upgrade

The following is a list of important notes and warnings about the upgrade process and changes in SPS 6.1.

CAUTION:

- **X.509 host certificates are not supported, the related options have been removed from the product. One Identity recommends using public keys instead.**
- **DSA keys are not supported, the related options have been removed from the product. One Identity recommends using RSA keys instead.**
- **The log ingestion feature of SPS has been removed from the product.**

CAUTION:

Due to a change in the underlying database, the upgrade process removes all risk scores generated earlier by One Identity Safeguard for Privileged Analytics. Sessions initiated after the upgrade will be scored again.

CAUTION:

As part of the upgrade, SPS upgrades its session database. This involves the following processes:

- **The first phase of the upgrade happens before SPS boots up and takes about 10-20 minutes. During this time, no production traffic goes through SPS, and SPS functionality is inaccessible. Rebooting or shutting down SPS at this stage of the upgrade may result in data loss. You can check the status of the upgrade process through either the console or the boot-time HTTP server, which allows you to view boot console log messages through your browser.**
- **Depending on the size of the session database, the second phase can take several days or even weeks to finish. You can check the status of the upgrade process through the System Monitor on the web interface of SPS.**

  This second phase of the upgrade is running in the background and consumes minimal resources. All functionality of SPS is accessible and SPS works as normal. The only limitation during this phase is that the session database used when searching on the REST API and the new Search interface is incomplete. The upgrade process starts with the most recent sessions and works its way backward in time until it reaches the oldest sessions. The classic search is unaffected.

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

CAUTION:

Following the upgrade, support for less than 1024-bit SSH keys is lost.

CAUTION:

When the client uses hostname in inband destination selections, the hostname must comply with RFC5890: Internationalized Domain Names for Applications (IDNA). For example, from the ASCII characters only letters, digits, and the hyphen character is permitted.

Starting with version 6.1.0, SPS rejects connection requests where the hostname does not comply with RFC5890.

NOTE:

Due to legal reasons, installation packages of the external indexer application will be available only from the SPS web interface. After SPS versions 6.3 and 6.0.2 are released, the installation packages will be removed from our website.

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.

3

Upgrade path to SPS 6.1

Upgrading to SPS 6.1 is tested and supported using the following upgrade path:

- *The latest SPS 6 LTS maintenance version (for example, 6.0.x) -> SPS 6.1*

  Always upgrade to the latest available maintenance version of SPS 5 LTS before upgrading to SPS 6.1.

From older releases, upgrade to 6 LTS first. For details, see How to upgrade to One Identity Safeguard for Privileged Sessions 6 LTS.

Upgrading a single SPS node to 6.1

The following describes how to upgrade a standalone One Identity Safeguard for Privileged Sessions (SPS) node to version 6.1.

- If you want to upgrade an SPS high-availability cluster, see Upgrading an SPS high-availability cluster to 6.1.
- If you want to upgrade an SPS central search or central management cluster, see Upgrading an SPS central cluster to 6.1.

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 SPS 6.1 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 SPS version, import the configuration of your SPS into this VMware version, and perform the upgrade. If everything is working, perform the upgrade on the production system.**

To upgrade a standalone SPS node to version 6.1

1. Complete the prerequisites described in Prerequisites for upgrading SPS and upgrade SPS to the latest revision of the current version.
2. Login to your support portal.

   You need a new license file for every LTS release. If there is no license file for One Identity Safeguard for Privileged Sessions 6.1 under your account, contact our Licensing Team and **Request a license key for a new version**.
3. Download the SPS 6.1 firmware ISO file from the Downloads page.
4. Upload the latest 6.1 firmware ISO file to your SPS. For details, see "Upgrading One Identity Safeguard for Privileged Sessions (SPS)" in the Administration Guide.
5. Click **Test** for the new firmware to check if your configuration can be upgraded to

version 6.1. 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**.

6. If the upgrade test is successful, activate the firmware.
7. *Recommended step.* To help troubleshoot potential issues following the upgrade, collect and save system information (create a support bundle) now.

   Navigate to **Basic Settings > Troubleshooting > Create support bundle** and choose **Create support bundle**.
8. Navigate to **Basic Settings > System**.

   CAUTION:

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

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

   NOTE:

   If you are upgrading to version 6.1 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 6.1. So during the upgrade to version 6.1, 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 6.1, SPS 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.
9. After the reboot, login to the web interface.

CAUTION:

In case the SPS web interface is not available within 30 minutes of rebooting SPS, 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 SPS encounters a problem during the upgrade process and cannot revert to its original state, SPS performs the following actions:

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH-access to SPS, unless SPS is running in sealed mode. That way it is possible to access the logs of the upgrade process, which helps the 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.

10. Navigate to **Basic Settings > System > Version details** and verify that SPS is running version 6.1 of the firmware. If not, it means that the upgrade process did not complete properly and SPS performed a rollback to revert to the earlier firmware version. In this case, complete the following steps:
    a. Navigate to **Basic Settings > Troubleshooting > Create support bundle** and click **Create support bundle**.
    b. Save the resulting ZIP file.
    c. contact our 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.
11. (Optional) If SPS 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 because 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.
12. Upgrade your Safeguard Desktop Player installations to the latest version. For details, see Upgrading the Safeguard Desktop Player.
13. Upgrade your external indexer installations to the latest version. For details, see Upgrading the external indexer.

Upgrading the Safeguard Desktop Player

Upgrading the Safeguard Desktop Player application is only a simple installation process.

NOTE: 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.

You can download the Safeguard Desktop Player application from the Downloads page.

For more information, see Safeguard Desktop Player User Guide.

Upgrading the external indexer

The following describes how to upgrade the indexer application on your external indexer hosts.

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.

To upgrade the indexer application on your external indexer hosts

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 an SPS high-availability cluster to 6.1

The following describes how to upgrade a One Identity Safeguard for Privileged Sessions (SPS) high-availability cluster.

- If you want to upgrade a standalone One Identity Safeguard for Privileged Sessions (SPS) node, see Upgrading a single SPS node to 6.1.
- If you want to upgrade an SPS central search or central management cluster, see Upgrading an SPS central cluster to 6.1.

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 secondary node on through the IPMI interface. For details on configuring the IPMI interface, see "Out-of-band management of One Identity Safeguard for Privileged Sessions (SPS)" in the Administration Guide.

CAUTION:

- **After performing the upgrade, it is not possible to downgrade to the earlier version. Upgrading to SPS 6.1 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 SPS version, import the configuration of your SPS 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 SPS nodes unless explicitly instructed.

CAUTION:

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

To upgrade an SPS high-availability cluster

1. Complete the prerequisites described in Prerequisites for upgrading SPS and upgrade SPS to the latest revision of the current version.
2. Login to your support portal.

   You need a new license file for every LTS release. If there is no license file for One Identity Safeguard for Privileged Sessions 6.1 under your account, contact our Licensing Team and **Request a license key for a new version**.
3. Download the SPS 6.1 firmware ISO file from the Downloads page.
4. Upload the latest 6.1 firmware ISO file to your SPS. For details, see "Upgrading One Identity Safeguard for Privileged Sessions (SPS)" in the Administration Guide.
5. Click **Test** for the new firmware to check if your configuration can be upgraded to version 6.1. 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**.
6. If the upgrade test is successful, activate the firmware.
7. Wait until the new firmware is synchronized to the slave node. This is usually completed within 60 seconds.
8. Navigate to **Basic Settings > High availability & Nodes > Other node** and click **Shutdown** to power off the slave node.

   CAUTION:

   Do not power on the secondary node.
9. *Recommended step.* To help troubleshoot potential issues following the upgrade, collect and save system information (create a support bundle) now.

   Navigate to **Basic Settings > Troubleshooting > Create support bundle** and choose **Create support bundle**.
10. Navigate to **Basic Settings > System**.

    CAUTION:

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

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

    NOTE:

    If you are upgrading to version 6.1 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 6.1. So during the upgrade to version 6.1, 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 6.1, SPS 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.

11. After the reboot, login to the web interface.

    CAUTION:

    In case the SPS web interface is not available within 30 minutes of rebooting SPS, 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 SPS encounters a problem during the upgrade process and cannot revert to its original state, SPS performs the following actions:

    - Initializes the network interfaces using the already configured IP addresses.
    - Enables SSH-access to SPS, unless SPS is running in sealed mode. That way it is possible to access the logs of the upgrade process, which helps the 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.

12. Navigate to **Basic Settings > System > Version details** and verify that SPS is running version 6.1 of the firmware. If not, it means that the upgrade process did not complete properly and SPS performed a rollback to revert to the earlier firmware version. In this case, complete the following steps:
    a. Navigate to **Basic Settings > Troubleshooting > Create support bundle** and click **Create support bundle**.
    b. Save the resulting ZIP file.
    c. contact our 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.
13. (Optional) If SPS 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 because 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.

14. If rebooting the primary node has been successful, power up the secondary node through IPMI.

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

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

16. Upgrade your external indexer installations to the latest version. For details, see Upgrading the external indexer.

8

Upgrading an SPS central cluster to 6.1

The following describes how to upgrade One Identity Safeguard for Privileged Sessions (SPS) central search or central management cluster.

- If you want to upgrade a standalone One Identity Safeguard for Privileged Sessions (SPS) node, see Upgrading a single SPS node to 6.1.
- If you want to upgrade an SPS high-availability cluster, see Upgrading an SPS high-availability cluster to 6.1.

Prerequisites:

Reserve an adequate maintenance window to have time to upgrade every node of the cluster. Having different SPS versions in the cluster should be avoided in production environments. For details on the different cluster roles, see "Cluster roles" in the Administration Guide.

To upgrade an SPS cluster

1. Upgrade the nodes that have the Search Minion role. Note that until you complete upgrading the entire cluster, the already upgraded nodes cannot audit traffic. For details on upgrading a node, see Upgrading a single SPS node to 6.1.
2. Upgrade the other Managed Host nodes.
3. If the Central Management node is different from the Search Master node, upgrade the Central Management node.
4. Upgrade the Search Master node.

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 SPS encounters a problem during the upgrade process and cannot revert to its original state, SPS performs the following actions:

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH-access to SPS, unless SPS 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 SPS, 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