One Identity Safeguard for Privileged Sessions 7.2

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.

SPSUpgrade Guide
Updated - 16 February 2023, 11:18

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

Contents

Preface

Welcome to One Identity Safeguard for Privileged Sessions (SPS) version 7.2 and thank you for choosing our product. This document describes the upgrade process from existing SPS installations to SPS 7.2. 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 7.2 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):

One Identity Safeguard for Privileged Sessions customers choose between two paths for receiving SPS releases: Long Term Supported (LTS) release or feature release.

Releases

	LTS release	Feature release
Release frequency	**Frequency**: Typically, every 2 years **Scope**: Includes new features, resolved issues and security updates **Versioning**: First digit identifies the LTS and the second digit is a 0 (for example, 6.0, 7.0, and so	**Frequency**: Typically, every 2 months **Scope**: Includes the latest features, resolved issues, and other updates, such as security patches for the OS **Versioning**: First digit identifies the LTS and the second digit is a number identifying the feature release (for example, 6.1, 6.2, and so on)

	on)	
Maintenance release	**Frequency**:Typically, every 2 months during full support **Scope**: Includes important resolved issues and security updates **Versioning**: Third digit designates the LTS maintenance release (for example, 6.0.1)	**Frequency**:Only for highly critical issues **Scope**: Includes highly critical resolved issues **Versioning**: Third digit designates the feature maintenance release (for example, 6.1.1)
Support	For more information on the product support, see Product Support - One Identity Safeguard for Privileged Sessions. For a full description of long-term-supported and feature releases, see Product Life Cycle & Policies - One Identity Safeguard for Privileged Sessions.	

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 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.

  NOTE: Version 2.2.0 and later of the One Identity Starling Two-Factor Authentication plugin works only if you have joined your SPS deployment to Starling.

  If you want use version 2.2.0 and later of the One Identity Starling Two-Factor Authentication plugin, complete the "Starling integration" in the Administration Guide procedure before upgrading the plugin.

Notes and warnings about the upgrade

The following is a list of important notes and warnings about the upgrade process and changes in SPS 7.2.

CAUTION:

After upgrading to version 7.0 LTS, SPS requires a new license. To avoid possible downtimes due to certain features not being available, before starting the upgrade, ensure that you have a valid SPS license for 7.0 LTS.

Upgrade as follows:

1. **Perform the upgrade to 7.0 LTS with your current license.**
2. **Update your SPS license to 7.0 LTS.**

For a new SPS license for 7.0 LTS, contact our Licensing Team.

CAUTION: From SPS version 6.12.0, the PAA database is also backed up as a part of the backup and restore procedure. Depending on the size of the PAA database, the backup size may increase significantly.

CAUTION: SPS support for Internet Explorer 11 (IE11) will soon be phased out.

SPS version 6.11.0 and previous versions continue to support IE11.

CAUTION:

After SPS 6.5, CentOS 6 operating systems will not be supported for external indexers. This means that after upgrading to SPS 6.5, or the LTS maintanance release in that cadence, you will not be able to use your external indexers that are running on CentOS 6. Make sure that you prepare your affected systems for this change and upgrade to CentOS 7 or later.

CAUTION:

SPS checks if the certificate revocation list (CRL) has expired and that the CRL has been signed by the same certificate authority (CA).

CAUTION: From version 6.8, SPS changes authenticating the users of the web interface with X.509 client certificates: certificates are validated against a trust store instead of a trusted CA list. During the upgrade, the trusted CA list formerly used for authentication is copied to a trust store that has revocation check disabled by default.

If you have previously enabled revocation check for your trusted CA list and already added the URLs of Certificate Revocation Lists (CRL), or you want to enable revocation check, you must edit the trust store settings manually.

- **Navigate to Basic Settings > Trust Stores.**
- **Select the revocation check type Leaf or Full for the trust store.**
- **Add a CRL URL for each root and intermediate CA.**

For more information about trust stores and how to configure them, see "Verifying certificates with Certificate Authorities using trust stores" in the Administration Guide.

CAUTION:

Make sure to check the value configured in Disk space fill-up prevention before starting the upgrade process. From SPS version 6.4, the value range of Disconnect clients when disks are: x percent used field in Basic Settings > Management > Disk space fill up prevention is limited to 50-98 percent. If your configured value is outside this range, you cannot start upgrading.

CAUTION:

Upgrading to SPS 6.3.0 and later versions involves a reorganization in the internal data storage of SPS. As a result, several files are moved to new location during the upgrade process. Depending on the amount of data (logs, index files, reports, and so on) stored on the appliance, this can take a long time, usually at least 30 minutes. When you activate the new firmware file, an estimate will be displayed.

To avoid data loss, the appliance will not boot if this step of the upgrade fails. In this case, contact our Support Team.

CAUTION:

Upgrading to SPS requires at least 10% free disk space.

Increase the amount of free disk space. For details, read Increasing the amount of available free disk space.

If increasing the amount of free disk space fails, or you encounter a different issue, contact our Support Team.

NOTE: Version 2.2.0 and later of the One Identity Starling Two-Factor Authentication plugin works only if you have joined your SPS deployment to Starling.

If you want use version 2.2.0 and later of the One Identity Starling Two-Factor Authentication plugin, complete the "Starling integration" in the Administration Guide procedure before upgrading the plugin.

CAUTION:

If you are authenticating your SPS users to an LDAP/Active Directory server, make sure that the response timeout of the LDAP/Active Directory server is at least 120 seconds.

CAUTION:

- **For SSH connections, X.509 host certificates are not supported, the related options have been removed from the product. One Identity recommends using public keys instead.**
- **For SSH connections, DSA keys are not supported, the related options have been removed from the product. One Identity recommends using RSA or Ed25519 keys instead.**
- **The log ingestion feature of SPS has been removed from the product.**

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 6.4 and 6.0.3 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 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.

CAUTION:

Starting from 6.10.0, SPS (SPS) has changed to hardened SSL settings. As a result, during TLS session establishment, the following items are not considered secure:

- **Private keys and X.509 certificates having RSA or DSA keys shorter than 2048 bits, or ECC keys shorter than 224 bits.**
- **Certificates (other than Root CA certificates) with signatures that use the SHA-1 or the MD5 hashing algorithm.**

With the hardened SSL settings, SPS will not connect to remote systems that are protected with weak certificates.

You cannot upgrade SPS if your configuration contains insecure certificates, keys or certificate chains in any of the following sections:

- **SPS web interface**
- **internal CA certificate**
- **connection policy TLS settings**
- **client X.509 credentials for external LDAP, SMTP or Syslog connections**
- **server X.509 certificates for external SMTP or Splunk servers**
- **external indexer credentials (only writable over the REST API)**
- **CA certificates in Trusted CA Lists and Trust Stores**

Note that the certificates and keys that are used for signing, timestamping, encryption or decryption are not affected by this change.

The accuracy of replaying audit trails in Asian languages (Traditional Chinese, Korean) has been enhanced. Due to this change, when upgrading SPS to version 6.11.0, all your sessions will be reindexed, and while reindexing is in progress, your sessions on the Search interface are incomplete. For this reason, plan your upgrade to SPS 6.11.0 accordingly.

Default Network Level Authentication (NLA) settings

Starting from 6.8.0, the default protocol-level settings for RDP connections have changed and NLA is now enabled by default in the RDP setting policies.

Due to this change:

- The default RDP setting is now **default_nla**, where NLA is enabled.
- The RDP setting, which was previously called default has been renamed to **legacy_default**.
- RDP 4-style authentication is now cleared by default.

NOTE: If you are upgrading from an SPS version earlier than 6.8.0, and you have an existing RDP setting named **legacy_default** or **default_nla**, you must rename it before upgrade.

Change the deprecated SHA1 signed certificates to SHA256 for RDP

CAUTION: If you are using SHA1 (Secure Hash Algorithm 1) signed certificates, SPS does not allow Remote Desktop Protocol (RDP) connections to Windows Servers.

Use the Microsoft Management Console (MMC) to verify your certificate:

- **If Remote Desktop Services (RDS) uses a self-signed certificate, make sure that you update your system to the latest patch level, then delete the certificate and restart the Remote Desktop Configuration service in order to re-generate the self-signed certificate.**
- **If RDS is using a certificate imported from a Public Key Infrastructure (PKI), contact your PKI admin for a new SHA256 certificate.**

3

Upgrade path to SPS 7.2

Upgrading to SPS 7.2 is tested and supported from the following versions:

- SPS 7 LTS.
- SPS 7.0.1.

To upgrade from SPS versions older than 7 LTS, first upgrade to 7 LTS. For details, see One Identity Safeguard for Privileged Sessions 7 LTS - Upgrade Guide.

Downgrading is not supported.

Upgrading a single SPS node to 7.2

The following describes how to upgrade a standalone One Identity Safeguard for Privileged Sessions (SPS) node to version 7.2.

- If you want to upgrade an SPS high-availability cluster, see Upgrading an SPS high-availability cluster to 7.2.
- If you want to upgrade an SPS central search or central management cluster, see Upgrading an SPS central cluster to 7.2.

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 7.2 is an irreversible process.**

To upgrade a standalone SPS node to version 7.2

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 7.2 under your account, contact our Licensing Team and **Request a license key for a new version**.
3. Download the SPS 7.2 firmware ISO file from the Downloads page.

   On the support portal, navigate to **Support > Download Software > One Identity Safeguard for Privileged Sessions** and download the latest install cdrom ISO file under **Application**.
4. Verify the integrity of the SPS 7.2 firmware ISO file with the hash available on the Downloads page.

CAUTION:Do NOT upgrade until you verify the integrity of the ISO file.

Verifying the integrity and authenticity of the ISO file is to make sure that it is not corrupted and it has not been tampered with by any other party. Verifying the ISO file guarantees that it has been officially released by One Identity.

NOTE: You can use the following utilities for hash verification (optional):

- On Unix systems: sha256sum.
- On Windows: Get-FileHash.

On Windows:

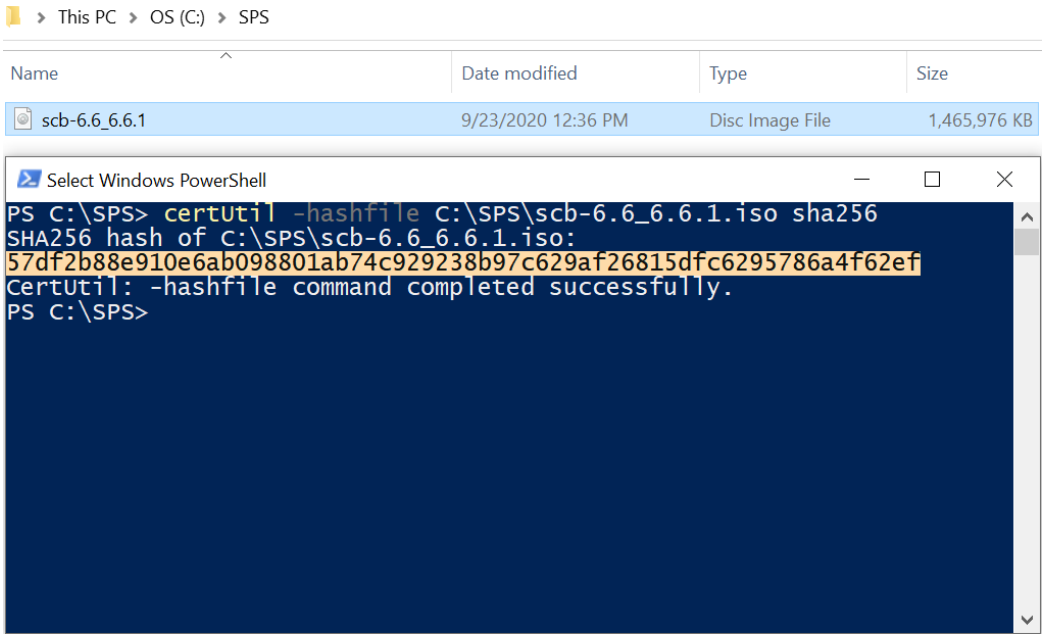
a. On your PC, navigate to the folder where you downloaded the ISO file.

b. Press and hold the **Shift** key.

c. Right-click in the folder and select **Open PowerShell window here**.

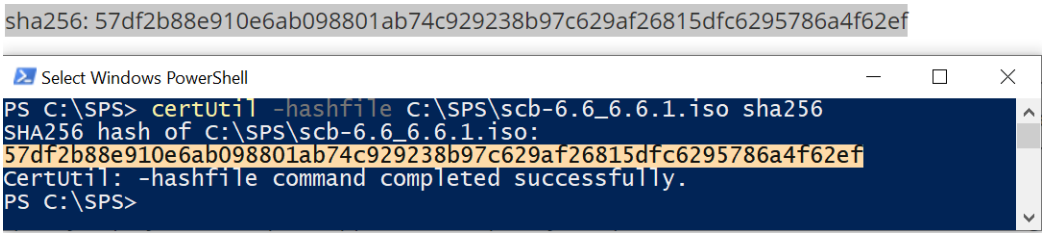
d. In the PowerShell window, enter the `certUtil -hashfile <path\to\sps.iso> sha256` command.

Figure 1: Example hash of the downloaded ISO file



e. Compare the hash of the file to the hash available on the Downloads page page: under **Application**, click **One Identity Safeguard for Privileged Sessions install cdrom**.

Figure 2: Example hash from the Support Portal



f. If the two hashes match, continue the upgrading process.

5. Upload the latest 7.2 firmware ISO file to your SPS. For details, see "Upgrading One Identity Safeguard for Privileged Sessions (SPS)" in the Administration Guide.
6. Click **Test** for the new firmware to check if your configuration can be upgraded to version 7.2. 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**.
7. If the upgrade test is successful, activate the firmware.
8. *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**.
9. 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 7.2 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 7.2. So during the upgrade to version 7.2, 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 7.2, 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.**

10. 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.

11. Navigate to **Basic Settings > System > Version details** and verify that SPS is running version 7.2 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.

12. (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.

13. Upgrade your Credential Store or other plugins to the latest version. You can download official plugins from Downloads page and upload them to SPS on the **Basic Settings > Plugins > Upload/Update Plugins** page.
14. Upgrade your Safeguard Desktop Player installations to the latest version. For details, see Upgrading the Safeguard Desktop Player.
15. Upgrade your external indexer installations to the latest version. For details, see Upgrading the external indexer.

5

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

This section describes how to upgrade the indexer application on your external indexer hosts.

CAUTION:

After SPS 6.5, CentOS 6 operating systems will not be supported for external indexers. This means that after upgrading to SPS 6.5, or the LTS maintanance release in that cadence, you will not be able to use your external indexers that are running on CentOS 6. Make sure that you prepare your affected systems for this change and upgrade to CentOS 7 or later.

NOTE: The version of the external indexer must be equal to or greater than the version of One Identity Safeguard for Privileged Sessions (SPS). To make sure you meet this criterion, One Identity recommends that you always upgrade your external indexer when you upgrade SPS. You can check that SPS has established a connection to the external indexer on the **Indexer** > **Worker status** page of the SPS web interface.

Prerequisites

Before you start, create a backup copy of the `/etc/indexer/indexerworker.cfg` and `/etc/indexer/indexer-certs.cfg` indexer configuration files. After SPS 6.13, the `/etc/indexer/indexer-certs.cfg` indexer configuration file is automatically renamed to `/etc/indexer/indexer-keys.cfg`.

To upgrade the indexer application on your external indexer hosts

1. Download the latest indexer `.rpm` package from the **Basic Settings > Local Services > Indexer service** page of the SPS web interface.

   NOTE: Due to legal reasons, installation packages of the external indexer application will be available only from the SPS web interface. After SPS versions 6.4 and 6.0.3 are released, the installation packages will be removed from our website.

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 7.2

CAUTION:

Creating a High-availability (HA) node pair from different types of hardware is not possible. The primary and the secondary HA nodes have to run on the same type of hardware.

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 7.2.
- If you want to upgrade an SPS central search or central management cluster, see Upgrading an SPS central cluster to 7.2.

Prerequisites:

Make sure that you have physically connected the IPMI to the network and that it is properly configured. This is important because you can only power the secondary node on through the IPMI. For details on configuring the IPMI, 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 7.2 is an irreversible process.**

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 7.2 under your account, contact our Licensing Team and **Request a license key for a new version**.
3. Download the SPS 7.2 firmware ISO file from the Downloads page.

   On the support portal, navigate to **Support > Download Software > One Identity Safeguard for Privileged Sessions** and download the latest install cdrom ISO file under **Application**.
4. Verify the integrity of the SPS 7.2 firmware ISO file with the hash available on the Downloads page.

   > **CAUTION:Do NOT upgrade until you verify the integrity of the ISO file.**
   >
   > **Verifying the integrity and authenticity of the ISO file is to make sure that it is not corrupted and it has not been tampered with by any other party. Verifying the ISO file guarantees that it has been officially released by One Identity.**

   > NOTE: You can use the following utilities for hash verification (optional):
   >
   > - On Unix systems: sha256sum.
   > - On Windows: Get-FileHash.

   On Windows:

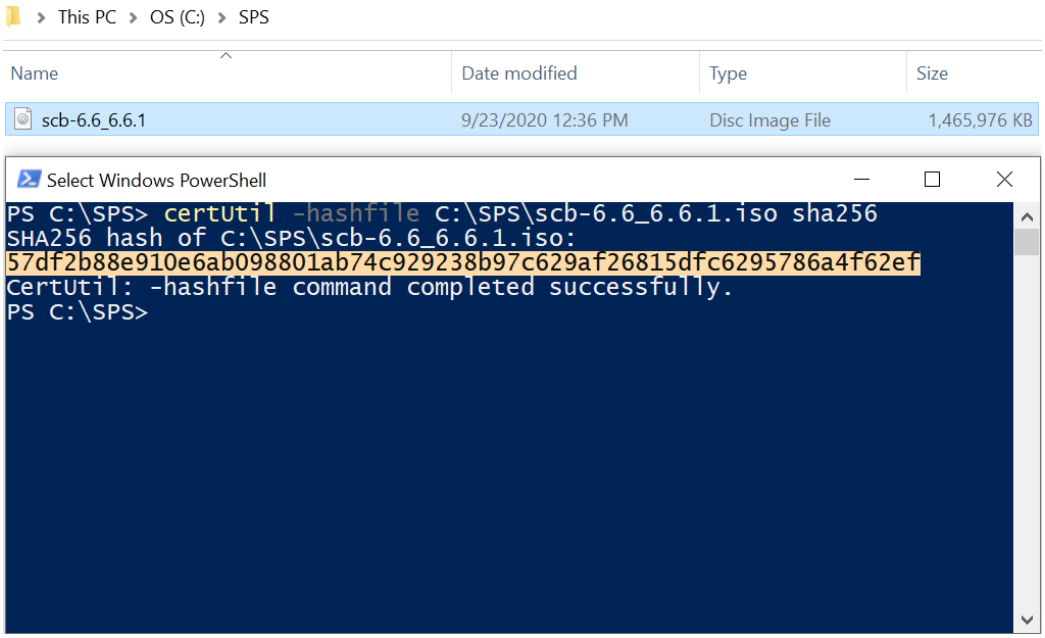
   a. On your PC, navigate to the folder where you downloaded the ISO file.

   b. Press and hold the **Shift** key.

   c. Right-click in the folder and select **Open PowerShell window here**.

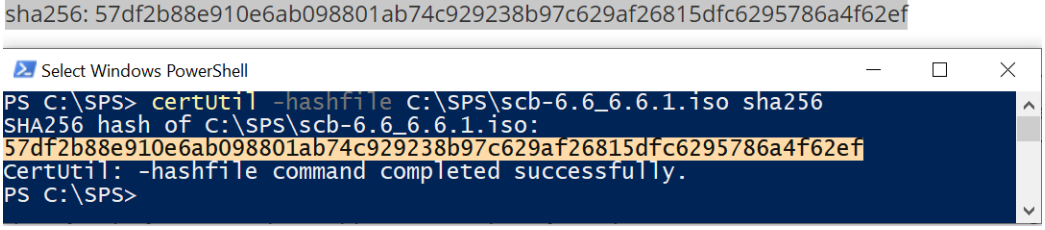
   d. In the PowerShell window, enter the `certUtil -hashfile <path\to\sps.iso> sha256` command.

Figure 3: Example hash of the downloaded ISO file



e. Compare the hash of the file to the hash available on the Downloads page page: under **Application**, click **One Identity Safeguard for Privileged Sessions install cdrom**.

Figure 4: Example hash from the Support Portal



f. If the two hashes match, continue the upgrading process.

5. Upload the latest 7.2 firmware ISO file to your SPS. For details, see "Upgrading One Identity Safeguard for Privileged Sessions (SPS)" in the Administration Guide.
6. Click **Test** for the new firmware to check if your configuration can be upgraded to version 7.2. 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**.
7. If the upgrade test is successful, activate the firmware.
8. Wait until the new firmware is synchronized to the slave node. This is usually completed within 60 seconds.

9. 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.

10. *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**.

11. 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 7.2 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 7.2. So during the upgrade to version 7.2, 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 7.2, 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.

12. 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.

13. Navigate to **Basic Settings > System > Version details** and verify that SPS is running version 7.2 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.
14. (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.
15. 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. This process is finished when the **Basic Settings > High availability & Nodes > Other node** appears.

    Note that at this stage, on the **Other node > Firmware version**, the version number next to **Current** is lower than the version number next to **After reboot**.
16. Click **Activate Slave**. This effectively turns the previously secondary node into the primary node. This process can take a few minutes.

    CAUTION:

    Do not skip this step! To run the Core firmware on the secondary node that you want to turn into the primary node, always click Activate Slave.

To ensure that the process is finished correctly, check the version numbers next to **Current** and **After reboot** on both the primary and the secondary node. These version numbers should all be the same. If the page is not refreshed after the process is finished, press **F5** to refresh the page.

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

Upgrading an SPS central cluster to 7.2

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 7.2.
- If you want to upgrade an SPS high-availability cluster, see Upgrading an SPS high-availability cluster to 7.2.

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 7.2.
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.

Increasing the amount of available free disk space

Upgrading to One Identity Safeguard for Privileged Sessions (SPS) requires at least 10% free disk space.

You can use one of the following methods to increase the amount of available free disk space.

NOTE: One Identity strongly recommends that you do not attempt any manual modifications to your configuration via SSH. Instead, use one of the following methods, or contact our Support Team.

Method to keep existing data

To increase the amount of available free disk space and keep existing data, create an archive policy at Policies > Backup & Archive > Archive policies.

For further information, see Archiving.

Method to delete existing data

To increase the amount of available free disk space by deleting existing data

1. Navigate to one of the following options:
   - **<Protocol name> Control** > **Global options**.
   - **<Protocol name> Control** > **Connections**.

   In the **Delete search metadata from SPS after** field, enter how long (in days) SPS must keep the `.zat` file and the metadata of sessions.

   For further information, see Configuring cleanup for the One Identity Safeguard for Privileged Sessions (SPS) connection database.

Method to increase the disk size of an SPS virtual appliance

If you are using an SPS virtual appliance, see "Modifying the disk size of a SPS virtual appliance" in the Installation Guide.

About us

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

Contacting us

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

Technical support resources

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

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

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