One Identity Safeguard for Privileged Sessions 5 LTS

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 - November 2018
Version - 5 LTS

Contents

Preface

Welcome to One Identity Safeguard for Privileged Sessions (SPS) version 5 LTS and thank you for choosing our product. This document describes the upgrade process from existing SPS installations to SPS 5 LTS. 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 5 LTS and Audit Player 2016.1 products.

Versions and releases of SPS

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

- *Long Term Supported or LTS releases* (for example, SPS 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, SPS 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, SPS 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.

3

Prerequisites for upgrading SPS

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

- You must have a valid software subscription to be able to download the new version of SPS, and also the new license file.
- You will need a support portal account to download the required ISO image / and the license. 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 One Identity Safeguard for Privileged Sessions - Technical Documentation.
- Export your configuration.

  For more information, see One Identity Safeguard for Privileged Sessions - Technical Documentation.
- 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 SPS T4 and T10, see the X9 SMT IPMI User's Guide. For SPS 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 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).

Notes and warnings about the upgrade

The following is a list of important notes and warnings about the upgrade process and changes in SPS 5 LTS.

Upgrading from SPS 4.0.9 or later:

CAUTION:

Upgrading the external indexers:

If you are using external indexers to process your audit trails, you must also upgrade your external indexer hosts. For details, see Upgrading the external indexer.

CAUTION:

The Audit Player indexer service has been deprecated and is not supported from SPS 4 F4. Before upgrading, you must configure SPS to use the Indexer service running on SPS, or install and configure external indexers.

For details, see Configuring external indexers in the Administration Guide.

If you need help to estimate the required number and resources of the external indexers, contact our Support Team.

Enabling the indexer without any previous estimations is dangerous and might result in overloading the box.

The indexer does not support USB Hardware security modules (HSMs). If your audit trails are encrypted and the related private keys are stored on a HSM, DO NOT UPGRADE to SPS 4 F4 or later.

CAUTION:

SPS now strictly checks if you have a High Availability license when running SPS in High Availability mode. You cannot upgrade to 4 F4 or later when using a single-node license in a HA environment. After upgrading to 4 F4 or later, an SPS node can be converted to HA only if a valid HA license is installed. (You can check your license at https://support.oneidentity.com/contact-us/licensing, or upload the 4 F4 firmware and select Basic Settings > System > Firmwares > Test firmware). Please, contact support if you perform the upgrade from version 4.0.6 or earlier. If you encounter any issues, contact our Support Team

To buy a valid HA license, contact your sales representative or contact our sales department

CAUTION:

When upgrading an SPS virtual appliance, make sure that the virtual machine has at least 4 GiB of memory. The recommended size for the memory depends on the exact environment, but consider the following:

- **The base system requires 4 GiB.**
- **SPS requires about 1-5 MiB of memory for every active connection, depending on the type of the connection — graphical protocols require more memory.**

CAUTION:

Handling of MAC addresses in High Availability clusters:

From SPS 4 F2, the MAC address of the interfaces will be different on the HA nodes, which means that during HA failover the MAC address for the configured IP addresses will change and no MAC address will be taken over to the slave node. This change will be propagated in Layer 2 by sending Gratuitous ARP requests, informing every host on that Local network about this change.

CAUTION:

Configuration of Append Domains field has changed:

Previous versions of SPS always implicitly assumed the Primary Search Domain (Basic Settings > Network) as an Append Domain in Inband Destination Selection settings of Connection policies, even when a custom DNS Server was set up for the connection. This behavior was changed in SPS version 4 F2: the Primary Search Domain is only used if no custom DNS Server is set. In order to not break existing configurations, the Primary Search Domain is set as an Append Domain explicitly for all affected policies during upgrade. If this is not the desired behavior for you, remove that additional entry.

CAUTION:

Upgrading to SPS version 4 F2 or newer will automatically delete any older firmwares, except for the version that was running when the upgrade process was started.

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:

Router and Bastion modes are deprecated in SPS version 4 F1 and later. It is now the connection's configuration which determines if the connection is transparent or non-transparent.

Router mode configurations are migrated to 4 F2 as the following:

- **The external interface is available as logical interface *External* on *Physical interface 1*.**

  You can change its alias IP addresses in Basic Settings > Network > Interfaces.
- **The internal interface is available as logical interface *Internal* on *Physical interface 3*.**

  You can change its alias IP addresses in Basic Settings > Network > Interfaces.
- **Routing (IP forwarding) is enabled between the following interfaces: Internal-Internal, External-External, and External-Internal. You can**

alter these settings in Basic Settings > Network > IP forwarding.

NOTE:

External, Management, and Internal interfaces are deprecated in SPS 4 F1 and later. All three interfaces are available as physical interfaces, with SPS listening on Physical interface 1 (formerly External, labeled 1 or EXT) during the initial connection.

To configure connections to use an interface, you must create a logical interface first. Each physical interface can have its own set of logical interfaces. Each logical interface must have its own VLAN ID, and can have its own set of (alias) IP addresses and netmasks.

You can enable routing (IP forwarding) between logical interfaces, and direct management traffic to use a dedicated interface.

To limit access to the configuration of SPS, create a separate, users-only login address where the configuration options of SPS are not accessible.

For more information, see One Identity Safeguard for Privileged Sessions - Technical Documentation.

NOTE:

When upgrading to SPS version 4 F1 or later, usergroups that had privileges to access the **Basic Settings > Management** page (for example, the **basic-view** and **basic-write** usergroups) can automatically access the **Basic Settings > Local Services** page, because most configuration options from the **Basic Settings > Management** page have been moved to the **Basic Settings > Local Services** page.

The **Indexer > Options** and **Indexer > Key management** pages have been moved to the **Basic Settings > Local Services** page. Privileges related to these deleted pages are automatically deleted from the privileges of every usergroup. If a usergroup had access only to these pages, then the users of these groups cannot login to SPS, because they will not have the privilege to access to any page. Assign privileges to such usergroups as needed.

NOTE:

It is strongly recommended to have IPMI (ILOM) or console access to the SPS appliance during the upgrade process. During the upgrade, SPS displays information about the progress of the upgrade and any possible problems to the console.

Upgrading from SPS 4.3.3 or later:

CAUTION:

SPS now strictly checks if you have a High Availability license when running SPS in High Availability mode. You cannot upgrade to 4 F4 or later when using a single-node license in a HA environment. After upgrading to 4 F4 or later, an SPS node can be converted to HA only if a valid HA license is installed. (You can check your license at https://support.oneidentity.com/contact-us/licensing, or upload the 4 F4 firmware and select Basic Settings > System > Firmwares > Test

firmware). Please, contact support if you perform the upgrade from version 4.0.6 or earlier. If you encounter any issues, contact our Support Team

To buy a valid HA license, contact your sales representative or contact our sales department

CAUTION:

When upgrading an SPS virtual appliance, make sure that the virtual machine has at least 4 GiB of memory. The recommended size for the memory depends on the exact environment, but consider the following:

- **The base system requires 4 GiB.**
- **SPS requires about 1-5 MiB of memory for every active connection, depending on the type of the connection — graphical protocols require more memory.**

CAUTION:

The Audit Player indexer service has been deprecated and is not supported from SPS 4 F4. Before upgrading, you must configure SPS to use the Indexer service running on SPS, or install and configure external indexers.

For details, see Configuring external indexers in the Administration Guide.

If you need help to estimate the required number and resources of the external indexers, contact our Support Team.

Enabling the indexer without any previous estimations is dangerous and might result in overloading the box.

The indexer does not support USB Hardware security modules (HSMs). If your audit trails are encrypted and the related private keys are stored on a HSM, DO NOT UPGRADE to SPS 4 F4 or later.

CAUTION:

Upgrading the external indexers:

If you are using external indexers to process your audit trails, you must also upgrade your external indexer hosts. For details, see Upgrading the external indexer.

NOTE:

It is strongly recommended to have IPMI (ILOM) or console access to the SPS appliance during the upgrade process. During the upgrade, SPS displays information about the progress of the upgrade and any possible problems to the console.

Upgrade path to SPS 5 LTS

Upgrading to SPS 5 LTS is tested and supported using the following upgrade path:

- **SPS 4.0.9 or later -> SPS 5 LTS latest maintenance release**
- **SPS 4.3.3 or later (that is, 4.3.x) -> SPS 5 LTS latest maintenance release**
- **The previous three SPS 5 LTS maintenance releases -> SPS 5 LTS latest maintenance release**

Updating to the latest version

Purpose:

To upgrade SPS to the latest revision of the current version, for example, from 4.0.1 to 4.0.6, complete the following steps:

Steps:

1. Download the latest SPS ISO file from the One Identity Downloads page
2. Update the firmware of your SPS.

Upgrading to SPS 5 LTS

Purpose:

If you want to upgrade an SPS cluster, see Upgrading an SPS cluster to 5 LTS. To upgrade a standalone SPS node to version 5 LTS, complete the following steps.

Prerequisites:

Read the following warnings before starting the upgrade process.

CAUTION:

SPS now strictly checks if you have a High Availability license when running SPS in High Availability mode. You cannot upgrade to 4 F4 or later

when using a single-node license in a HA environment. After upgrading to 4 F4 or later, an SPS node can be converted to HA only if a valid HA license is installed. (You can check your license at https://support.oneidentity.com/contact-us/licensing, or upload the 4 F4 firmware and select Basic Settings > System > Firmwares > Test firmware). Please, contact support if you perform the upgrade from version 4.0.6 or earlier. If you encounter any issues, contact our Support Team

To buy a valid HA license, contact your sales representative or contact our sales department.

CAUTION:

- **After performing the upgrade, it is not possible to downgrade to the earlier version. Upgrading to SPS 5 LTS is an irreversible process.**
- **Certain configuration options were removed from SPS 4 F1. Before upgrading, you might have to change your configuration to ensure that it can be upgraded.**
- **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:

The Audit Player indexer service has been deprecated and is not supported from SPS 4 F4. Before upgrading, you must configure SPS to use the Indexer service running on SPS, or install and configure external indexers.

For details, see Configuring the internal indexer and Configuring external indexers in the Administration Guide.

If you need help to estimate the required number and resources of the external indexers, contact our Support Team.

Enabling the indexer without any previous estimations is dangerous and might result in overloading the box.

The indexer does not support USB Hardware security modules (HSMs). If your audit trails are encrypted and the related private keys are stored on a HSM, DO NOT UPGRADE to SPS 4 F4 or later.

Steps:

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 account.

   NOTE:

If you have update subscription included in support, you can use your original LTS license file.

3. Download the SPS 5 LTS firmware files from the One Identity Downloads page.
4. Upload the latest 5 LTS firmware files to your SPS.
5. Click **Test** for the new firmware to check if your configuration can be upgraded to version 5 LTS. If the test returns any errors, correct them before continuing the upgrade process. If you encounter any problems, contact the One Identity Support Team.

   Select **After reboot**.

   Local User Databases cannot be used for server-side authentication in SPS version 4 F1 and newer. For server-side authentication, use a local Credential Store. If your configuration contains server-side elements in a Local User Database, complete One Identity Safeguard for Privileged Sessions - Technical Documentation before upgrading to SPS version 4 F1 or newer.

   CAUTION:

   Proceed only if the upgrade test is successful.
6. Activate the firmware.
7. *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 > System debug** and choose **Collect and save current system state info**.

   CAUTION:

   Do NOT click Reboot cluster during the upgrade process unless explicitly instructed.
8. Navigate to **Basic Settings > System > 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 to the local console.

   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 LTS, 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.

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 Message field. Click View.

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

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

9.

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 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.

10. Navigate to **Basic Settings > System > Version details** and verify that SPS is running version 5 LTS 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 > System debug** and click **Collect and save current system state info**.
    b. Save the resulting ZIP file.
    c. Next, 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. **Note.** Skip this step if you have upgraded to SPS version 4.1.1 or later.

    Complete the following steps if you have upgraded to SPS version 4.1.0, and all the following points are true to your configuration:

    - You have configured at least one IP alias on the external interface of SPS.
    - SPS was running in Bastion or Nontransparent mode.
    - The **Basic Settings > Management > SSH settings > Enable remote SSH access** was set.
    - There was a connection policy in **SSH Control > Connections** that had one of the external interface IP addresses (or a network that includes such IP addresses) set in its **To** field, and 22 in its **Port** field.

    If the above points are all true to your configuration, then the connections of the connection policy will fail after the upgrade, because during the upgrade, every IP address of the interfaces that had the **Permit administrator login** set were added

to the **Basic Settings > Local Services > SSH Server > Listening addresses** list. To solve the problem, delete the unneeded IP address from the **Basic Settings > Local Services > SSH Server > Listening addresses**. Typically, you will need to delete every address except the first one.

12. Upgrade your Audit Player installations to the latest version. For details, see the section called “Upgrading the Audit Player”.

Upgrading the Audit Player

Upgrading the Audit Player application (AP) is only a simple installation process. See the One Identity Safeguard for Privileged Sessions 5 LTS Administrator Guide for details. The Audit Player application can be downloaded from the One Identity Downloads page.

Upgrading the external indexer

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

1. Download the latest indexer package from the One Identity 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 cluster to 5 LTS

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 One Identity Safeguard for Privileged Sessions - Technical Documentation.

Purpose:

To upgrade an SPS high-availability cluster, complete the following steps.

CAUTION:

- **After performing the upgrade, it is not possible to downgrade to the earlier version. Upgrading to SPS 5 LTS is an irreversible process.**
- **Certain configuration options were removed from SPS 4 F1. Before upgrading, you might have to change your configuration to ensure that it can be upgraded.**
- **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.

Steps:

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 account.

   NOTE:

   If you have update subscription included in support, you can use your original LTS license file.
3. Download the SPS 5 LTS firmware files from the One Identity Downloads page.
4. Upload the latest 5 LTS firmware files to your SPS.
5. Wait until the new firmware is synchronized to the slave node. This is usually

completed within 60 seconds.

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

   Select **After reboot**.

   Local User Databases cannot be used for server-side authentication in SPS version 4 F1 and newer. For server-side authentication, use a local Credential Store. If your configuration contains server-side elements in a Local User Database, complete One Identity Safeguard for Privileged Sessions - Technical Documentation before upgrading to SPS version 4 F1 or newer.

7. **CAUTION:**

   Proceed only 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 debug bundle) now.

   Navigate to **Basic Settings > Troubleshooting > System debug** and choose **Collect and save current system state info**.

9. Navigate to **Basic Settings > High availability & Nodes > Other node** and click **Shutdown** to power off the slave node.

10. **CAUTION:**

    Do not power on the slave node.

    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. 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 to the local console.

    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 LTS, 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.

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 Message field. Click View.**

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

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

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.

11.

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 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.

12. Navigate to **Basic Settings > System > Version details** and verify that SPS is running version 5 LTS 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 > System debug** and click **Collect and save current system state info**.
    b. Save the resulting ZIP file.
    c. Next, 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. If the master reboot has been successful, power up the slave node through IPMI.
14. **Note.** Skip this step if you have upgraded to SPS version 4.1.1 or later.

    Complete the following steps if you have upgraded to SPS version 4.1.0, and all the following points are true to your configuration:

    - You have configured at least one IP alias on the external interface of SPS.
    - SPS was running in Bastion or Nontransparent mode.
    - The **Basic Settings > Management > SSH settings > Enable remote SSH access** was set.
    - There was a connection policy in **SSH Control > Connections** that had one of the external interface IP addresses (or a network that includes such IP addresses) set in its **To** field, and 22 in its **Port** field.

    If the above points are all true to your configuration, then the connections of the connection policy will fail after the upgrade, because during the upgrade, every IP

address of the interfaces that had the **Permit administrator login** set were added to the **Basic Settings > Local Services > SSH Server > Listening addresses** list. To solve the problem, delete the unneeded IP address from the **Basic Settings > Local Services > SSH Server > Listening addresses**. Typically, you will need to delete every address except the first one.

15. If SPS is functioning properly after the upgrade, power up the slave node through the IPMI 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.

16. Upgrade your Audit Player installations to the latest version. For details, see the section called "Upgrading the Audit Player".

Migrating a Local User Database to local Credential Store

Purpose:

Local User Databases cannot be used for server-side authentication in SPS version 4 F1 and newer. For server-side authentication, you have to use a local Credential Store. If your configuration contains server-side elements in a Local User Database, you have to complete the following steps before upgrading to SPS version 4 F1 or newer.

Prerequisites:

Update your SPS to version 4.0.6 or a later 4.0.x version. The script required to migrate a Local User Database to local Credential Store is not available in earlier versions.

Steps:

1. Login to the SPS web interface.
2. Create an empty, local Credential Store. For details, see One Identity Safeguard for Privileged Sessions - Technical Documentation.
3. If you have created a password-protected Credential Store in the previous step, navigate to **Unlock Credential Store**, select the Credential Store, enter the password, then click **Unlock**.
4. Login to SPS via a local console, or remotely using SSH.
5. Execute the following command: `/opt/SPS/bin/lud-to-credstore-migrator.php <name-of-local-user-database> <name-of-empty-credential-store>`

   This will migrate the server-side credentials from the Local User Database to an existing, but empty Credential Store. If a user in the Local User Database has no client-side credentials (hence would have no credentials at all after the migration), then the whole user entry will be deleted from the Local User Database.

6. Check all of your RDP, SSH and Telnet Connection policies. For every Connection

policy that has an Authentication policy configured which uses the Local User Database you migrated in the previous step, complete the following steps:

   a. In the Connection Policy, select the Credential Store you created in Step 2.

   b. If you do not use the Local User Database for client-side authentication, delete it from the Authentication policy.

7. Complete this procedure for any other Local User Database that contains server-side elements (that is, **Policies > Local User Databases > Server Side (private key/certificate)** contains any keys or certificates).
8. Perform any other configuration change you need before upgrading to SPS 4 F1.

6

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