How to upgrade to Balabit's Privileged Session Management 5 F6

June 19, 2018

Abstract
Upgrade Guide for Balabit's Privileged Session Management (PSM)

Table of Contents

1. Preface

Welcome to Balabit's Privileged Session Management (PSM) version 5 F6 and thank you for choosing our product. This document describes the upgrade process from existing PSM installations to PSM 5 F6. The main goal of this paper is to help system administrators in planning the migration to the new version of PSM.

Warning
Read the entire document thoroughly before starting the upgrade.

This document covers the Balabit's Privileged Session Management 5 F6 product.

1.1. Versions and releases of PSM

As of June 2011, the following release policy applies to Balabit's Privileged Session Management:

- *Long Term Supported or LTS releases* (for example, PSM 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, PSM 4.0.1). Maintenance releases to LTS releases contain only bugfixes and security updates.
- *Feature releases* (for example, PSM 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, see the *Balabit version policy*.

Warning
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.

All questions, comments or inquiries should be directed to <info@balabit.com> or by post to the following address: One Identity LLC 1117 Budapest, Alíz Str. 2 Phone: +36 1 398 6700 Fax: +36 1 208 0875 Web: *https://www.balabit.com/*

2. Prerequisites for upgrading PSM

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

- You must have a valid software subscription to be able to download the new version of PSM, and also the new license file.
- You will need a *MyDownloads* 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 *Section 4.7, Data and configuration backups* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- Export your configuration.
  For more information, see *Procedure 6.4.5, Exporting the configuration of PSM* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.
- Verify that PSM 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 PSM T4 and T10, see the *X9 SMT IPMI User's Guide*. For PSM 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 PSM 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 PSM 5 F6.

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

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

If there are any errors during the upgrade, *contact the One Identity Support Team*.

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

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

Warning
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 the One Identity Support Team*.

Upgrading from PSM 5.0.0 or later:

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

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

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

1. Login to PSM.
2. Navigate to **Basic Settings > Troubleshooting > System debug**, click **COLLECT AND SAVE CURRENT SYSTEM STATE INFO**, and save the file.
3. Open *https://support.balabit.com/* and click **Submit a Ticket**.
4. In the **Type of request** field, select **Request for information**.
5. Into the **Subject** field, enter `Determining hardware type`.
6. Click **Add File**, and upload the file you downloaded from PSM in Step 1.
7. We will check the type of your hardware and notify you.

3. Upgrade path to PSM 5 F6

Upgrading to PSM 5 F6 is tested and supported using the following upgrade path:

- **The latest PSM 5 LTS maintenance version (for example, 5.0.x) -> PSM 5 F6**
  Always upgrade to the latest available maintenance version of PSM 5 LTS before upgrading to PSM 5 F6.

- **The latest maintenance versions of the previous three feature releases (in this case, PSM 5 F3 or later) -> PSM 5 F6**
  Always upgrade to the latest available maintenance version of the feature release before upgrading to PSM 5 F6.

From older releases, upgrade to 5 LTS first. For details, see *How to upgrade to Balabit's Privileged Session Management 5 LTS*.

4. Procedure – Upgrading to PSM 5 F6

Purpose:

If you want to upgrade a PSM cluster, see *Procedure 7, Upgrading a PSM cluster to 5 F6 (p. 10)*. To upgrade a standalone PSM node to version 5 F6, complete the following steps.

Prerequisites:

Read the following warnings before starting the upgrade process.

Warning

- After performing the upgrade, it is not possible to downgrade to the earlier version. Upgrading to PSM 5 F6 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 PSM version, import the configuration of your PSM into this VMware version, and perform the upgrade. If everything is working, perform the upgrade on the production system.

Steps:

Step 1. Complete the prerequisites described in *Section 2, Prerequisites for upgrading PSM (p. 4)* and upgrade PSM to the latest revision of the current version.

Step 2. Login to your *MyBalabit account*.

Step 3. Download the PSM 5 F6 firmware files from the *One Identity Downloads page*.

Step 4. Upload the latest 5 F6 firmware files to your PSM. For details, see *Upgrading PSM* in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.

Step 5. Click **Test** for the new firmware to check if your configuration can be upgraded to version 5 F6. 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**.

Step 6.

Warning
Proceed only if the upgrade test is successful.

Activate the firmware.

Step 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**.

Step 8.

Warning
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. PSM will start with the new firmware and upgrade its configuration, database, and other system components. During the upgrade process, PSM displays status information and other data on the local console and on the web interface of PSM, at any of the **Listening addresses** configured at **Basic settings > Local Services > Web login (admin and user)**.

Note
If you are upgrading to version 5 F6 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 5 F6. So during the upgrade to version 5 F6, you will not be able to see any upgrade logs on the web interface.

Warning
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.

Warning
After the reboot in 5 F6, PSM 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...
```

Step 9.

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

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

If there are any errors during the upgrade, *contact the One Identity Support Team*.

Step 10.

Warning
In case the PSM web interface is not available within 30 minutes of rebooting PSM, check the information displayed on the local console and *contact the One Identity 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 PSM encounters a problem during the upgrade process and cannot revert to its original state, PSM performs the following actions:

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

Step 11. Navigate to **Basic Settings > System > Version details** and verify that PSM is running version 5 F6 of the firmware. If not, it means that the upgrade process did not complete properly and PSM performed a rollback to revert to the earlier firmware version. In this case, complete the following steps:

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

Step b. Save the resulting ZIP file.

Step c. *Contact the One Identity Support Team* and send them the file. They will analyze its contents to determine why the upgrade was not completed and assist you in solving the problem.

Step 12. *Optional step:* If PSM was in a domain before the upgrade, navigate to **RDP Control -> Domain membership** and make sure that your domain-related settings are correct. In case of correct settings, you will see the following:

- **Fully qualified domain name (realm name): Host joined currently configured domain successfully.**
- **Currently joined domains:** `<name.of.the.joined.domain>`

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

Step 13. Upgrade your Safeguard Desktop Player installations to the latest version. For details, see *Section 5, Upgrading the Safeguard Desktop Player (p. 9)*.

5. Upgrading the Safeguard Desktop Player

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

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

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

6. Procedure – Upgrading the external indexer

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

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

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

Prerequisites:

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

Steps:

Step 1. Download the latest indexer package from the *One Identity Downloads page*.

Step 2. Copy the downloaded `.rpm` package to your external indexer hosts.

Step 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
```

Step 4. Execute the following command: `yum upgrade -y indexer.rpm`

Step 5. Resolve any warnings displayed during the upgrade process.

Step 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
```

Step 7. Repeat this procedure on every indexer host.

7. Procedure – Upgrading a PSM cluster to 5 F6

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 *Section 6.8, Out-of-band management of PSM* in *The Balabit's Privileged Session Management 5 F6 Administrator Guide*.

Purpose:

To upgrade a PSM high-availability cluster, complete the following steps.

Warning

- After performing the upgrade, it is not possible to downgrade to the earlier version. Upgrading to PSM 5 F6 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 PSM version, import the configuration of your PSM into this VMware version, and perform the upgrade. If everything is working, perform the upgrade on the production system.

Warning
Do NOT reboot any of the PSM nodes unless explicitly instructed.

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

Steps:

Step 1. Complete the prerequisites described in *Section 2, Prerequisites for upgrading PSM (p. 4)* and upgrade PSM to the latest revision of the current version.

Step 2. Login to your *MyBalabit account*.

Step 3. Download the PSM 5 F6 firmware files from the *One Identity Downloads page*.

Step 4. Upload the latest 5 F6 firmware files to your PSM. For details, see *Upgrading PSM* in *The Balabit's Privileged Session Management 5 LTS Administrator Guide*.

Step 5. Wait until the new firmware is synchronized to the slave node. This is usually completed within 60 seconds.

Step 6. Click **Test** for the new firmware to check if your configuration can be upgraded to version 5 F6. 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**.

Step 7. 

Warning
Proceed only if the upgrade test is successful.

Activate the firmware.

Step 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**.

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

Warning
Do not power on the slave node.

Step 10. 

Warning
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. PSM will start with the new firmware and upgrade its configuration, database, and other system components. During the upgrade process, PSM displays status information and other data on the local console and on the web interface of PSM, at any of the **Listening addresses** configured at **Basic settings > Local Services > Web login (admin and user)**.

Note
If you are upgrading to version 5 F6 from version 5.0.x, status information is displayed on the web interface only after the first boot to version 5 F6. So during the upgrade to version 5 F6, you will not be able to see any upgrade logs on the web interface.

Warning
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.

Warning
After the reboot in 5 F6, PSM 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...
```

Step 11.

Warning
In case the PSM web interface is not available within 30 minutes of rebooting PSM, check the information displayed on the local console and *contact the One Identity 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 PSM encounters a problem during the upgrade process and cannot revert to its original state, PSM performs the following actions:

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

Step 12. Navigate to **Basic Settings** > **System** > **Version details** and verify that PSM is running version 5 F6 of the firmware. If not, it means that the upgrade process did not complete properly and PSM performed a rollback to revert to the earlier firmware version. In this case, complete the following steps:

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

Step b. Save the resulting ZIP file.

Step c. *Contact the One Identity Support Team* and send them the file. They will analyze its contents to determine why the upgrade was not completed and assist you in solving the problem.

Step 13. If the master reboot has been successful, power up the slave node through IPMI.

Step 14.

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

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

If there are any errors during the upgrade, *contact the One Identity Support Team*.

Step 15. If PSM is functioning properly after the upgrade, power up the slave node through the IMPI web interface.
The slave node attempts to boot with the new firmware, and reconnects to the master node to sync data. During the sync process, certain services (including Heartbeat) are not available. Wait for the process to finish, and the slave node to boot fully.

Step 16. Upgrade your Safeguard Desktop Player installations to the latest version. For details, see *Section 5, Upgrading the Safeguard Desktop Player (p. 9)*.

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

- Initializes the network interfaces using the already configured IP addresses.
- Enables SSH-access to PSM, unless PSM 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 PSM, check the information displayed on the local console and *contact the One Identity Support Team*.