opentext™

OpenText Software Delivery Management

Software version: 25.1

Upgrade Guide for Linux

Go to Help Center online

https://admhelp.microfocus.com/octane/

Document release date: July 2025

Send Us Feedback

Let us know how we can improve your experience with the Upgrade Guide for Linux.

Send your email to: admdocteam@opentext.com

Legal Notices

Contents

Upgrade highlights

The following sections include specific highlights for upgrading from a given version.

General upgrade notes

Note the following general information when upgrading.

Category	Description
Backups	Make sure to have viable accessible backups of your relational database (either Oracle or SQL Server), Elasticsearch, and the repository folder on your file system.
Cluster	Make sure to stop services for all cluster nodes before upgrading.
STP/LTP Upgrade	You can choose between two upgrade paths: • **Short-term path (STP)**. Upgrade to each new service pack (for example, from 23.4 to 24.1). If you choose this path, you need to go through all the interim service packs to upgrade to the following release. • **Long-term path (LTP)**. Upgrade directly from one LTP release to the next (for example, from 16.2.100 directly to 24.3 and then to 25.1, the next LTP release), without having to upgrade to each of the interim service packs. Refer to the release's upgrade path details below.

Upgrade to 25.1 (LTP release)

Category	Description
Upgrade path	This version is an LTP release. You can upgrade to this version directly from 24.3 (the previous LTP release).
Harden the authentication	You must harden the authentication mechanism by replacing the existing **hpssoconfig.xml** configuration file and storing the encryption key in a keystore file. For details, see "Harden the authentication" in the 25.1 Upgrade Guide.

Upgrade to 24.3 (LTP release)

Note the following when upgrading to 24.3 (LTP release).

Category	Description
Upgrade path	This version is an LTP release. You can upgrade to this version directly from 16.2.100 (the previous LTP release), or from 24.1.

Category	Description
Java version	JDK 21 is required and must be installed before you upgrade. Before you install JDK 21, make a backup copy of the default Java keystore (**cacerts**) file from the existing JDK 11 installation. Then, after you install JDK 21, use the backup copy to replace the **cacerts** file that is provided with JDK 21. This avoids potential issues with the new **cacerts** file.
Elasticsearch version	Elasticsearch 8.11 or later is required (version 8.11 is recommended). This is enforced on startup.
Elasticsearch re-index	The upgrade triggers Elasticsearch re-index. Indexes are re-indexed to version 8. When a space's post-upgrader is running, its Elasticsearch features are not all disabled during the entire process. Instead, features are in downtime only when an index they are dependent on is in the downtime phase of its re-indexing. For details, see "Upgrade highlights" on page 3. **Note:** Re-index must be completed successfully, or you cannot upgrade to the next release.
OData version	OData 4.0 is required. OData version 2.0 services will no longer work and will be fully replaced by OData version 4.0. To continue using OData, your connection must be updated to OData version 4.0. The OData 4.0 URI format is: <https://<server>/odata/**v4**/shared_spaces/<space_ID>/workspaces/<workspace_ID>/

Upgrade to 24.1

Note the following when upgrading to 24.1.

Category	Description
Upgrade path	This version is an STP service pack, meaning that you can only upgrade to 24.1 from 23.4. If you have not yet upgraded to 23.4, upgrade now.
Elasticsearch version	Elasticsearch 8.x is required. This is enforced on startup.

Upgrade to 23.4

Note the following when upgrading to 23.4.

Category	Description
Upgrade path	This version is an STP service pack, meaning that you can only upgrade to 23.4 from 16.2.100. If you have not yet upgraded to 16.2.100, upgrade now.

Upgrade to 16.2.100 (LTP release)

Note the following when upgrading to 16.2.100 (LTP release).

Category	Description
Upgrade path	This version is a long term path (LTP) release, meaning that you can upgrade to 16.2.100 either directly from 16.1.100, or from 16.1.200.
Elasticsearch version	Elasticsearch 8.6.0 is now supported. We recommend using Elasticsearch 7.17.8 or 8.6.0.
Elasticsearch re-index	If you are upgrading directly from 16.1.100, verify that re-index has completed successfully in all spaces. For details, see "LTP Path: Verify Elasticsearch re-indexing (ES version 8.x)" in the 16.2.100 Upgrade Guide.
MS SQL Server databases	If you are using MS SQL Server databases with the FILL_ EXISTING site_action, the database administrator should set READ_COMMITTED_SNAPSHOT ON on all databases used by OpenText Software Delivery Management, before deploying the new version. For details, see "Changes to MS SQL Server databases" in the 16.2.100 Upgrade Guide.

Upgrade to 16.1.200

Note the following when upgrading to 16.1.200.

Category	Description
Upgrade path	This version is an STP service pack, meaning that you can only upgrade to 16.1.200 from 16.1.100. If you have not yet upgraded to 16.1.100, upgrade now.
Elasticsearch re-index	In this service pack, Elasticsearch re-index is mandatory. • **Space re-index.** Spaces that have not been re-indexed are not accessible to users. You must complete re-index before upgrading. If you do not, you can re-index after upgrading, but access to the shared space is blocked until re-index is completed successfully. • **Site re-index.** Re-index is not enforced at the site level. It is the responsibility of the site admin to verify that site re-index is complete. If re-index is not complete, the index will not perform properly following upgrade. For example, audit data may be inaccurate. In addition, upgrade to Elasticsearch 8 may fail in future releases.

Upgrade to 16.1.100 (LTP release)

Note the following when upgrading to 16.1.100 (LTP release).

Category	Description
Upgrade path	This version is a long term path (LTP) release, meaning that you can upgrade to 16.1.100 either directly from 16.0.100, or from 16.0.400.

Category	Description
Elasticsearch re-index	The upgrade triggers Elasticsearch re-index. It is important to note that the mechanism for Elasticsearch re-index has been changed to significantly minimize downtime. When a space's post-upgrader is running, its Elasticsearch features are not all disabled during the entire process. Instead, features are in downtime only when an index they are dependent on is in the downtime phase of its re-indexing. For details, see "Prepare for Elasticsearch re-indexing" in the 16.1.100 Upgrade Guide. Note that re-index must be completed. You will not be able to use OpenText Software Delivery Management in the next release if re-index was not completed successfully.
Hazelcast version	16.1.100 uses Hazelcast v.5.1. This requires changes to the hazelcast.xml configuration file. For details, see "Update the hazelcast.xml configuration file" in the 16.1.100 Upgrade Guide.
Docker support	You can now use OpenText Software Delivery Management in Docker. For details, see "Upgrade OpenText Software Delivery Management in Docker" in the 16.1.100 Upgrade Guide.
Known issue	When upgrading to 16.1.100 directly from 16.0.100 (LTP upgrade path) in Oracle environments, if you have a space with more than 500 workspaces, you may encounter an error message regarding the **FixVulnerabilitiesCountOfWIUpgrader** Data upgrader. For a workaround, see “Troubleshooting a Data upgrader failure” in the 16.1.100 Upgrade Guide.

Upgrade

This document describes how to upgrade an existing installation of an on-premises OpenText™ Software Delivery Management server on Linux.

This section includes:

Upgrade paths

You can choose between two upgrade paths:

- **Short-term path (STP)**. Upgrade to each new service pack (for example, from 23.4 to 24.1). If you choose this path, you need to go through all the interim service packs to upgrade to the following release.
- **Long-term path (LTP)**. Upgrade directly from one LTP release to the next (for example, from 16.2.100 directly to 24.3 and then to 25.1, the next LTP release), without having to upgrade to each of the interim service packs.

This version is an LTP release. You can upgrade to this version directly from 24.3 (the previous LTP release).

Prerequisites

Before upgrading, note the following:

- JDK 21 is required and must be installed before you upgrade.

  Before you install JDK 21, make a backup copy of the default Java keystore (**cacerts**) file from the existing JDK 11 installation. Then, after you install JDK 21, use the backup copy to replace the **cacerts** file that is provided with JDK 21. This avoids potential issues with the new **cacerts** file.

- Elasticsearch 8.11 or later is required (version 8.11 is recommended). This is enforced on startup.

- The upgrade triggers Elasticsearch re-index. Indexes are re-indexed to version 8.

  When a space's post-upgrader is running, its Elasticsearch features are not all disabled during the entire process. Instead, features are in downtime only when an index they are dependent on is in the downtime phase of its re-indexing.

  For details, see "Upgrade" on the previous page.

  > **Note:** Re-index must be completed successfully, or you cannot upgrade to the next release.

- OData 4.0 is required. OData version 2.0 services will no longer work and will be fully replaced by OData version 4.0.

  To continue using OData, your connection must be updated to OData version 4.0. The OData 4.0 URI format is:

  <https://<server>/odata/**v4**/shared_spaces/<space_ID>/workspaces/<workspace_ID>/

Prepare for upgrade

Before upgrading, review the following:

1. Check that all spaces are up to date, first in **Settings > Site > Spaces**, and then in **Settings > Site > POST UPGRADE JOBS.** Delete any spaces that you do not want to upgrade to prevent problems in future upgrades.
2. Verify that your server machine, and if relevant, all cluster nodes, meet all prerequisites.

   This includes checking the supported versions for all third party tools such as Elasticsearch, and upgrading accordingly. For details, see "Prerequisites" in the *Installation Guide for Linux*.
3. Stop the **octane** service on the server, and if relevant, on all cluster nodes.
4. Create backups of:
   - The repository
   - Existing configuration files, including **octane.conf**
   - Your database
   - Elasticsearch
5. Take note of any special aspects of your configuration.

Special configuration	Recommendation
Did you use a different user, other than the **octane** user, to install?	If you did, the user is set in the **OCTANE_USER** environment variable. Use this user to upgrade.
Did you install to a location other than **/opt/octane**?	Refer to the location that you used while upgrading.
What sudoer user did you use to install?	Use the same sudoer user that was used for installation to upgrade.

Special configuration	Recommendation
Did your organization's DBA make changes to database schemas, such as adding tables or columns?	Define an exception file. The exception file instructs OpenText Software Delivery Management to ignore manual changes to the database schemas during installation. For details, see "Using exception files for manual database changes" in the *Installation Guide for Linux*.

6. Before upgrading, remove all patches or hotfixes at **WEB-INF/lib** and **WEB-INF/classes.**

   Example of a full path for Linux environment:

   - **/opt/octane/webapps/root/WEB-INF/classes**
   - **/opt/octane/webapps/root/WEB-INF/lib**

Step 1: Deploy the new version and start the server

1. Download the OpenText Software Delivery Management RPM package:

   https://sld.microfocus.com/mysoftware/download/downloadCenter

2. Deploy the RPM package for the new version of OpenText Software Delivery Management:

   ```
   rpm -Uvh --prefix <install-path> <name of new rpm file>
   ```

   > **Note:** If the rpm command fails on Java version, see https://softwaresupport.softwaregrp.com/doc/KM000023838.

3. Harden the authentication.

   a. Create a backup of the existing **hpssoconfig.xml**configuration file.

   b. In the repository folder, rename the existing **hpssoconfig.xml**configuration file in the repository folder to **hpssoconfig.xml.old**.

   c. Rename the **hpssoconfig.xml.new** file to **hpssoconfig.xml**.

> **Note:** Make sure that the repository is defined with the same path in all the nodes. The keystore path is defined as an absolute path. Therefore, it is important that all server nodes look for the key in the same location.

d. Store the encryption key in a keystore file.

You can use the automatically generated keystore or provide your own keystore. For details, see "Harden the authentication" on the next page.

4. Update the configuration files in the **conf** and **osp-config** folders, as follows.

Item	Details
osp-config folder	Perform the following steps regarding the **<repository folder>/conf/osp-config** folder: a. If any of the files in the folder were manually modified, copy the changes into the corresponding files in the **osp-config.new** folder. b. Rename the **osp-config** folder to **osp-config.old**. c. Rename the **osp-config.new** folder to **osp-config**.
.conf files	Perform the following steps regarding files In the **<repository folder>/conf/** folder: a. If any of the **.conf** files were manually modified, merge the changes into the corresponding **.conf.new** files. b. Rename all the **.conf** files to **.conf.old**. c. Rename all the **.conf.new** files to **.conf**.

5. Start the OpenText Software Delivery Management server:

```
systemctl start octane
```

6. Check the **/opt/octane/log/wrapper.log** file. If you encounter a recoverable error in the **wrapper.log** or **upgrade.log** files, fix the problem and restart the server to resume upgrade.

- The following is required if you configured trust on the OpenText Software Delivery Management server, when connecting to a remote location such as the database server. If your Java trust store (**<java_home>/jre/lib/security/cacerts**) uses a non-default password, enter this password in **octane.conf** in the **java-default-trust-store-password** parameter.

Caution: Do not use OpenText Software Delivery Management until you have completed "Step 3: Upgrade spaces" on the next page.

Harden the authentication

This version uses a stronger encryption mechanism, which requires changes to the **hpssoconfig.xml** configuration file. You must harden the authentication mechanism by replacing the existing **hpssoconfig.xml** configuration file with the new file provided, and storing the encryption key in a keystore file.

You can use the automatically generated keystore or provide your own keystore.

- By default, if you do not provide a keystore, a keystore is automatically generated during the first server start up and placed in the configuration folder. The keystore is randomly generated and unique for each individual installation, to ensure security.
- If you provide your own keystore, only BKS format is supported, and the keystore should contain a 256-bit AES key.

  Add the following information to the **octane.conf** file:

```
hp-sso{
    # the entry name inside keystore
    keystore-cipher-alias = “<alias>”
    # password to open the key inside keystore
    keystore-cipher-alias-password = “<alias password>”
    # Absolute path to the keystore
    keystore-location = “<absolute keystore path>”
    # password to open the keystore
    keystore-password = “<keystore password>”
}
```

Note:

- You can define a subset of parameters, such as the passwords. The defined parameters are used and any missing parameters are generated.
- If you do not define all the parameters, the keystore path is overridden with the path to the generated keystore.

Step 2: Upgrade cluster nodes

After the upgrade on the first node has completed successfully, you can upgrade the remaining nodes in a cluster.

To upgrade cluster nodes:

1. Deploy the new version of OpenText Software Delivery Management to each node.
2. On each node, start the OpenText Software Delivery Management server.

   ```
   systemctl start octane
   ```

3. Check the **/opt/octane/log/wrapper.log** file. If you do not see the "Server is ready!" message, correct the errors shown in the log.

   If you encounter a recoverable error in the **wrapper.log** or **upgrade.log** files, fix the problem and restart the server to resume upgrade.

Caution: Do not use OpenText Software Delivery Management until you have completed "Step 3: Upgrade spaces" below.

Step 3: Upgrade spaces

After upgrading, log in as the site admin to upgrade each space.

To upgrade spaces:

1. In a browser, go to **<*ServerURL*>:<*port*>/ui/?site**.
2. Log in with the user name and password defined in the **octane.conf** file.

   To upgrade all spaces at once, log in as the site admin.
3. Click **Site** and then click the **Spaces** tab.

4. Select one or more spaces and click **Upgrade**.

   Upgrade is available only if the space needs to be upgraded.

5. Individual workspaces are upgraded in the background.

> **Note:** Some data might be unavailable in trend graphs and other Elasticsearch-related features until all of the post-upgrade jobs have completed.

Step 4: Verify that spaces upgraded successfully

Verify that all spaces were upgraded successfully from the previous version. To verify that a space has been upgraded, check that:

- The space status is **Active** (or Inactive if it was previously deactivated).
- The space version is updated to the current version.

In addition, check that all post-upgrade jobs were completed in **Settings > Site > POST UPGRADE JOBS**.

Rollback

This section describes how to roll back after upgrading an on-premises OpenText Software Delivery Management server. This may be necessary if for some reason the upgrade fails or performance is slow.

Depending on when you want to roll back, there are different steps to perform.

> **Note:** To roll back you need the pre-upgrade backups of all configuration files including **octane.conf** from each node.

This section includes:

After the upgrade's setup validation phase

You can roll back after the upgrade's setup validation phase, whether it passed or failed.

If the upgrade reached setup validation, the following have been modified:

- Previously-deployed files
- Configuration files, including **octane.conf**

To roll back the deployed files, including octane.conf:

1. Revert to the previous rpm file: `rpm -Uvh --oldpackage <filename>`
2. Revert to backups of configuration files, including **octane.conf**.
3. Start the OpenText Software Delivery Management server (the octane service).

After a site schema has been upgraded

You can roll back after the site schema has been upgraded.

If the upgrade upgraded the site schema, the following have been modified:

- The site schema (database)
- Elasticsearch indexes
- Configuration files, including **octane.conf**

To roll back the site schema:

1. Stop the OpenText Software Delivery Management server (the octane service).
2. Revert to a backup of the site schema.
3. Revert to a backup of Elasticsearch indexes.
4. Revert to the previous rpm file: `rpm -Uvh --oldpackage <filename>`
5. Revert to backups of configuration files, including **octane.conf**.
6. Start the OpenText Software Delivery Management server (the octane service).

After space schema has been upgraded

If the upgrade upgraded the space schema, the following have been modified:

- Previously-deployed files
- Elasticsearch indexes
- Configuration files, including **octane.conf**
- The site schema
- The space schema

Rolling back a single space is relevant after upgrade of a space failed. In this case, fixes are required depending on the cause of the failure, as seen in the logs and in the UI.

> **Note:** This is only relevant if the space upgrade failed with **CORRUPTED** status. If it ended in **SUSPENDED** status, implement the fixes as instructed in the logs and in the UI, and then resume upgrade. No rollback actions are required.

To roll back changes to the space schema:

1. Revert to the backup of the space schema.
2. Revert to the backups of Elasticsearch indexes related to the specific space.

   Space-specific indexes can be identified by the space logical name embedded in their name, using the pattern **mqm_{space logical name}_***.

   > **Note:** There are multiple Elasticsearch indexes for each space. Make sure to roll back all of them.

3. Revert to the repository backup of this specific space.
4. Fix what caused the upgrade to fail.
5. Run the following API to repair the space:

   ```
   POST {octane server}/admin/shared_spaces/repair?ids={space_id}
   ```

   > **Tip:** To repair multiple spaces, provide the **space_ids** separated by commas.

6. Upgrade again.

After upgrade completed

If the upgrade completed successfully, the following have been modified:

- Configuration files, including **octane.conf**
- The site schema
- The space schema(s)
- Elasticsearch indexes
- Repository files

To roll back the entire upgrade:

1. Follow the procedure "To roll back the site schema:" on the previous page.
2. Revert to backups of all space schemas.
3. Revert to backups of all Elasticsearch indexes.
4. Revert to backup of the previous repository.

After upgrading cluster nodes

If you upgraded additional cluster nodes, the following have been modified on the cluster nodes:

- Previously-deployed files
- Configuration files, including **octane.conf**

To roll back to the **rpm** package:

1. Revert to the previous **rpm** file on each cluster node: `rpm -Uvh --oldpackage <filename>`
2. Revert to backups of configuration files, including **octane.conf**.
3. Start the OpenText Software Delivery Management server (the octane service) on each cluster node.

Upgrade in Docker

This section describes how to upgrade OpenText Software Delivery Management in Docker.

This section includes:

Get default configuration files from the docker image

Before upgrading, make sure you have default configuration files from the new OpenText Software Delivery Management Docker image.

1. Download the new OpenText Software Delivery Management Docker image.
2. Run the Docker image using the following command:

```
docker run -d -p 8080:8080 -v /opt/octane_docker_config_
files/conf:/opt/octane/conf -v /opt/octane_docker_config_
files/log:/opt/octane/log -v /opt/octane_docker_config_
files/repo:/opt/octane/repo --name alm_octane_config_files
lifecyclemanagement/octane:<version_number>
```

   The first run should fail with errors because OpenText Software Delivery Management has not been configured.
3. Go to **/opt/octane_docker_config_files/repo**. The **conf-discover** folder contains the default configuration files. Copy them to a backup location.

Upgrade in Docker

This section describes how to start a new OpenText Software Delivery Management container using the configuration from a previous version, and upgrade the data.

1. Stop your OpenText Software Delivery Management container.
2. Back up your Oracle or MSSQL database.

3. Back up Elasticsearch.
4. Back up the conf and log folders (if mapped).
5. Back up the REPO folder, which includes the **conf-discover** and **storage** folders.
6. Download the new OpenText Software Delivery Management Docker image.

   Note that only on-premises versions of OpenText Software Delivery Management are supported.
7. Overwrite the .xml files in the folder **conf-discover** (in the REPO folder) with the .xml files from the default configuration files for the new version. For details see "Get default configuration files from the docker image" on the previous page.
8. Harden the authentication by storing the encryption key in a keystore file. The authentication mechanism uses a stronger encryption algorithm.

   You can provide your own keystore or use the automatically generated keystore.

   - If you use your own keystore, only BKS format is supported, and the keystore should contain a 256-bit AES key.

     Add the following information to the **octane.conf** file:

     ```
     hp-sso{
         # the entry name inside keystore
         keystore-cipher-alias = “<alias>”
         # password to open the key inside keystore
         keystore-cipher-alias-password = “<alias password>”
         # Absolute path to the keystore
         keystore-location = “<absolute keystore path>”
         # password to open the keystore
         keystore-password = “<keystore password>”
     }
     ```

   - If you do not provide a keystore, a keystore is automatically generated during the first server start up and placed in the configuration folder.

> **Note:**
> - You can define a subset of parameters, such as the passwords. The defined parameters are used and any missing parameters are generated.
> - If you do not define all the parameters, the keystore path is overridden with the path to the generated keystore.

9. Update the configuration files in the **conf** and **osp-config** folders, as follows.

Item	Details
osp-config folder	Perform the following steps regarding the **<repository folder>/conf/osp-config** folder: a. If any of the files in the folder were manually modified, copy the changes into the corresponding files in the **osp-config.new** folder. b. Rename the **osp-config** folder to **osp-config.old**. c. Rename the **osp-config.new** folder to **osp-config**.
.conf files	Perform the following steps regarding files In the **<repository folder>/conf/** folder: a. If any of the **.conf** files were manually modified, merge the changes into the corresponding **.conf.new** files. b. Rename all the **.conf** files to **.conf.old**. c. Rename all the **.conf.new** files to **.conf**.

10. Run the Docker image with the following command, using the identical container configuration:

```
docker run -d -p 8080:8080 -p 8443:8443 -v [your-path-to-CONF-
folder]:/opt/octane/conf -v [your-path-to-LOG-
folder]:/opt/octane/log -v [your-path-to-REPO-
folder]:/opt/octane/repo --name alm_octane_<version_number>
lifecyclemanagement/octane:<version_number>
```

This means that the ports, and the mapping of the conf, log, and repo mount folders should be the same in the new container as your current container.

11. Validate that the container works by checking the container's **Log** tab, or the **wrapper.log** and **octane.log** files in the mapped log folder.
12. Continue with the regular space upgrade procedure, as described in "Step 3: Upgrade spaces" on page 15.

Note: If you need to roll back the upgrade:

- If the new OpenText Software Delivery Management container failed to run, restore configuration files in the conf-discover folder (in the REPO folder), and run the previous version of the OpenText Software Delivery Management container.
- If the new OpenText Software Delivery Management container successfully upgraded the site, restore backups (database, Elasticsearch, and REPO folder), and run the previous version of the OpenText Software Delivery Management container.

Install a patch

This section describes how to install a hotfix patch, without upgrading OpenText Software Delivery Management.

1. Stop the OpenText Software Delivery Management service.
2. Create backups of:
   - The repository
   - Existing configuration files, including **octane.conf**
   - Your database
   - Elasticsearch
3. Run the installer file containing the fix as you would do for a regular upgrade.
4. Start the OpenText Software Delivery Management service and validate that the issue is fixed.

   There is no need to upgrade the spaces.