A MITEL
PRODUCT
GUIDE

Unify OpenScape Composer

OpenScape Composer V2

Administration Guide
09/2024

A31003-X3020-M100-27-76A9

Mitel

Notices

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Europe Limited. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes. No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos, and graphics (collectively “Trademarks”) appearing on Mitel’s Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively “Mitel), Unify Software and Solutions GmbH & Co. KG or its affiliates (collectively “Unify”) or others. Use of the Trademarks is prohibited without the express consent from Mitel and/or Unify. Please contact our legal department at iplegal@mitel.com for additional information. For a list of the worldwide Mitel and Unify registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

Contents

1 General Information about the OpenScape Composer

This guide presents:

- the available features and how to operate them.
- guidelines for managing and monitoring the communications solution with OS Composer
- guidelines for backing up and restoring the configuration of your communication solution within OS Composer

1.1 Functional Range of OpenScape Composer

OS Composer is a web application, which provides the following features to the administrator:

- **Inventory**

  Using the inventory feature you get information on any problems concerning the applications (via Notifications) and perform administrative actions, such as taking an application Backup.
- **Software updates**

  Whenever an application update is available, OS Composer will notify the user, who will have to manually download and install any application updates.
- **Licenses**

  OS Composer displays a list of all the licenses being installed in each OpenScape application, notifying the administrator whenever a license is about to expire.
- **Certificates**

  OS Composer displays a list of all the certificates being installed in each OpenScape application, notifying the administrator whenever a certificate is about to expire.
- **Notifications**

  The various OpenScape system components create Notifications that are displayed in the Notifications section.
- **Backup and restore**

  The administrator can manually trigger a backup for one or more applications, or schedule a backup to be automatically executed (for example: every day, at 12:00) for all the applications.
- **Logs**

  OS Composer allows you to download log files from the different applications. To download more detailed log files, follow the steps below:

  1) Download the file: `/opt/cmpnext/app/cmpn_logback.xml`
  2) Edit the file by changing the log level value from INFO to DEBUG:

  ```
  <logger name="com.unify.cmp" additivity="false">
   <level value="DEBUG" />
  ```

  3) Restart OS Composer, by running the following commands:

```
$ systemctl stop cmpn
```

and

```
$ systemctl start cmpn
```

1.2 Requirements

Browser Requirements

OS Composer is currently optimized for Google Chrome and Mozilla Firefox.

Operating System Requirements

OS Composer can be installed on SUSE Linux Enterprise Server (SLES) 12 SP1 or later

2 Installation and Update

Execute the following commands to install the OS Composer

Installation

Follow the steps below to install OS Composer from console:

1) Place the `OpenScapeComposer-V*.tar.gz` file in a temporary directory on the server you want to install the OS Composer and execute the following commands from the directory where the `OpenScapeComposer-V*.tar.gz` is placed
2) Execute

   ```
   tar -xvf OpenScapeComposer-V1.R0.1.0.tar.gz
   ```

   The installation files are now unzipped.
3) Execute:.

   ```
   /deploy-composer.sh
   ```

   The OS Composer is installed.

   For more information on the `deploy-composer.sh` script, run:

   ```
   ./deploy-composer.sh -h
   ```

Update

Follow the steps below to update OS Composer from UI:

- Before updating
  - Enable **OSV Automatic Software Updates** from the **Features** setting, as described in Configuring General Options.

- Online update (Recommended when the Composer has internet access to SWS and can automatically download the software from SWS)

  1) Before starting the online update:

  – Fill in the proxy settings as described in Configuring General Options
  – Fill in the Software Update Settings, as described in Configuring General Options

  2) Click **<Current User>**

  3) Click **Update Composer…**

  4) Select **Online** (Automatic download from SWS) and click **Next**

  5) The latest Composer version will be shown, provided that the Composer is not already in latest version and there are no network issues.

  6) Select the HD (local) repository where the files will be downloaded.

  NOTICE:

  Remote repositories (SFTP and FTP) are not supported because the files need to be locally for the update

  7) Select the installation file that you have downloaded from SWS. This will be a *.tar.gz file. This is an optional step

  NOTICE:

  You can either upload the installation file here or directly to the repository. For large files (for example the .iso file used for the Live Upgrade), you must upload the file directly to the repository and leave this field blank.

  8) Click **Update**.

  9) Composer will automatically update itself. When it is ready, the page will reload and the login screen will be displayed.

  NOTICE:

  During the update process, the Composer will restart and become offline. Ensure that no other jobs are running during the update

- Offline update (Manual Download. Recommended only when the Composer does not have internet access to SWS and so cannot download the software automatically)

  1) Before starting the offline update:
  - Download manually the software bundle from SWS
  - Place the `.tar.gz` file in an HD repository on Composer (for example, the builtin repository at `/opt/cmpnext/BACKUPS)`
  - Keep the metadata .json file locally

  2) Click **<Current User>**
  3) Click **Update Composer…**
  4) Select **Offline update** (Manual Download) and click **Next**
  5) Select the HD (local) repository where you have placed the files.

  NOTICE:

  Remote repositories (SFTP and FTP) are not supported because the files need to be locally for the update

  6) Click **browse** and upload the metadata `.json` file
  7) Click **Update**
  8) Composer will automatically update itself. When it is ready the page will reload and the login screen will be displayed.

  NOTICE:

  During the update process, the Composer will restart and become offline. Ensure that no other jobs are running during the update

Updates, backup and restore

The `application-production.yml` file is a properties file that you can use to add or modify the existing application properties from the `application.yml` file. By using both files, all properties are loaded, with the `application-production.yml` properties overriding the default ones from `application.yml`.

During the update of the Composer, the `application-production.yml` file is backed up and restored so that the configuration is preserved after the update.

Uninstall Composer

```
% rpm -evh cmp-server-1.0.8.1

% rpm -evh orientdb-2.2.19-1.noarch

% rpm -evh ibm-java-x86_64-80_1.noarch
```

OrientDB service handling

```
% systemctl status -l orientdb - shows the status

% systemctl stop orientdb - stops the service

% systemctl start orientdb - starts the service
```

Handle CMP Next Server service

```
% systemctl status -l cmpn - shows the status

% systemctl stop cmpn - stops the service

% systemctl start cmpn - starts the service
```

3 Getting started

3.1 How to Log In to OpenScape Composer

Prerequisites

In order to log in to the OS Composer, you must have a user account that has been assigned administrator privileges.

Step by Step

1) Enter the following address in your web browser:
   `https://<server IP address>:8085/admin/login`

   NOTICE:

   For the OSEE V9, the IP address is the External IP address of the SBC THIG

2) In the **Username** field specify the ID of the user account with which you want to log on. Default is "operator".
3) Enter the associated password in the Password field. The default password is "Asd123!.". Change this password after your first login.

   NOTICE:

   You can click on the eye button next to the Password field to toggle password text visibility.

4) Click on **Sign in**.

   NOTICE:

   In case you want to Delete a user, you have to do it through the swagger API. The swagger API is accessed via entering the following url on your web-browser:

   `https://<server IP address>:8085/swagger-ui/index.html`

3.1.1 Operator password

Complexity rules of operator password

- The password can only contain printable ASCII characters except for space
- The password must be between 8 and 28 characters
- The password cannot include the username
- The password cannot be changed to the same as the previous password

- The password must contain at least one character from at least 3 of the following groups

  1) lowercase letters
  2) uppercase letters
  3) numbers
  4) special characters (e.g. @, !, $)

How to reset operator password

In case you have forgotten your password or been locked out from the OS Composer, follow the steps below to reset the operator password to the default one:

1) Add java to Path:

```
export JAVA_HOME=/opt/cmpnext/packages/ibm-java-x86_64-80/jre/
```

```
export PATH=$JAVA_HOME/bin:$PATH
```

2) Start orientdb console:

```
cd /opt/cmpnext/packages/orientdb-community/bin/
```

```
sh console.sh
```

3) Connect to `cmpn db`:

Connect remote:

`127.0.0.1/cmpn admin <admin_pswd>` (Default password is admin)

4) Update password:

```
update SystemUser set password = '$2a$10$Xp/UnnsZxzOHk.aE4.LOFecZjwRO9lr1cnkB1Nt05.UxuzD2Uu2Tm', passwordNeedsChange = 'true' where username = 'operator'
```

```
exit
```

The password is reset to `Asd123!.` and you must change it on your first login.

3.2 Before using the OpenScape Composer

Configure the settings described below.

Step by Step

1) Click the <**Current User**> button.
2) A dropdown menu appears with several options.
3) Click **Profile**. Give your email, for example: admin@cmpnx.com and OS Composer will be sending any notifications (for example, an application is down, or a license expires in one week) as e-mail messages to the administrator.

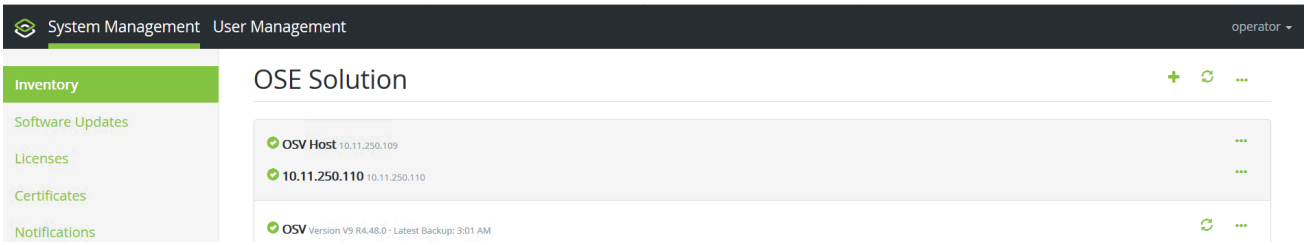
- Click **Change Password**. Give a new password and click **Save**.

3.3 About the User Interface

OS Composer user interface consists of HTML pages that can be accessed using a web browser. As a result OS Composer is platform-independent and can be operated using all prevalent operating systems.

The user interface is divided into the following areas:

1) Header
2) Navigation
3) Work area



3.3.1 Header

The header contains the following elements:

1) System Management

It can be used as a "home" button and redirect you back to the landing page.

2) User Management

Here you can manage the user accounts in your network and the services that these users can use.Click on the User Management element and the User List appears. This list shows all created users with their data:

- **Username**
- **E-mail address**
- **First name**
- **Last name**

Click the "**+**" to add a new user. A pop-up window appears with necessary settings for the new user:

- **First Name**: The new user's first name, for example *firstName*
- **Last Name**: The new user's last name, for example *lastName*
- **Username**: The new user's username, for example *admin*
- **Password**: The new user's password, for example *userSecretPassword*.
  - **Password needs change**: Check this checkbox to change the password.
  - **Password never expires**: Check this checkbox in order for the password to always remain the same.
- **Email**: The new user's email, for example *admin@cmpnx.com*

IMPORTANT:

Currently, OS Composer supports only the functionality to Add a new user. The Delete functionality can be completed using API requests from swagger and for the

Edit functionality, you have to add a new user with the updated settings and delete the old one.

3) Click on the <**Current User**> button. For detailed information, see Before using the OpenScape Composer.

3.4 Default Application Passwords

- Host Credentials
  - These are the credentials used to perform an SSH connection to the application. The credentials are different for each application.
  - For the Windows Applications (for example Xpressions, Deployment Server, Concierge, Contact Center, Trace Manager), the credentials used to login the Windows Server (for example username: administrator).

    NOTICE:

    You must install the OpenSSH server
  - For the OSV Application the srx password is required: 2GwN!gb4
  - For OSB Applications, the default credentials will be created automatically during synchronization. The default credentials are:

    Username: service

    password: BF0bpt@x
  - For SBC Applications, credentials need to be inserted manually (see the default credentials above).
- Application Credentials
  - UC & Media Server & Multiple Communication Server Admin: Api username: administrator@system, Password: "Asd123!."
  - DLS: Api username: api, Password: "Asd123!."

3.5 Host addition with Fully Qualified Domain Name (FQDN)

To add a host using an FQDN instead of its IP address, the OpenScape Composer needs to resolve said FQDN. This can be achieved either by adding a new entry to the `/etc/hosts` file or by setting up the DNS that is being utilized.

UC & Media Server & Multiple Communication Server Admin specific restrictions

When an FQDN was used during the initial setup of the application server, the same FQDN has to be used when adding the application on OS Composer. This FQDN needs to be added on the `/etc/hosts` file as well, as described above. When these changes are performed, if the application seems offline on the User Interface, restart the OS Composer by following the instructions on Start/Stop OpenScape Composer Server. The restart has to be executed only once after these changes.

4 Operating the OpenScape Composer

4.1 Configuring General Options

The OpenScape Composer allows you to configure general settings, download logs, received information etc.

Step by Step

1) Click the <**Current User**> button.

2) Click **Settings**. This option allows you to configure various settings of OS Composer:

a) **Email (SMTP)**: Enter an SMTP (Simple Mail Transfer Protocol) server, which will be used by OS Composer to send e-mail notifications to the administrator. Give the **SMTP URL**, for example *10.1.1.1:8080*, **SMTP username**, for example *admin* and the **SMTP password**, for example *smtpSecretPassword*.

b) **Email (Messages)**:

Configure the following parameters:

- **Minimum Severity Level**

  First select one of the following options from the dropdown list to set a threshold regarding the severity level of e-mail messages you want to receive, e.g. if you select 'Warning' as a minimum severity level, you will only receive e-mail messages for warnings and errors:

  – Info
  – Warning
  – Error

- **E-mail Message Types**

  Then select the type of e-mail messages you want to receive by clicking the toggle button on the right side of each option to turn off a particular message type.

  NOTICE: By default notification types are enabled. For example, if you toggle off **Certificates Expiration**, you will not receive a notification message for this type.

  Possible options are:

  – Node Status Changes
  – Backup/Restore jobs
  – Software Download/Update jobs
  – Licences Expiration
  – Certificates Expiration
  – SWS Latest Software Checks

  Click **Save** to save the changes.

c) **CoProxy**: Give the **Proxy FQDN or IP address**, for example `172.29.38.124`, **Proxy Port**, for example *8080*, **Proxy username**,

for example *admin* and **Proxy password**, for example *proxy-SecretPassword*.

d) **Software Updates**:

Configure the following parameters:

- – Give the **SWS URL**, for example.

```
https://sws.unify.com:447/SWSService4CSP/
SWService4CMP.asm?wsdl
```

The credentials are only needed during the OS Composer registration on the SWS server and they are not stored in the local database.

– Enter the **Siel ID**, e.g. *SID:mockSielID*.

NOTICE: Siel ID is stored in the local database.

– Enter your **Access Key Id** or **SWS Username** , e.g. *myAccessKeyId*.

– Enter your **Secret Access Key** or **SWS Password**, e.g. *mySecretAccessKey*.

NOTICE: In case **Access Key Id** and **Secret Access Key** are not available, login to SWS-WebService Portal and create SWS WebService account and credentials.

Click **Generate new** to generate the SWS certificate.

– For the **Customer Type** parameter, select a value from the drop-down menu: *Non Government (Civil) incl. Telecom*, *Military, Paramilitary, Police, Intelligence Services* or *Government without Telecom, Military, Paramilitary, Police, Intelligence*
.

– Select your **Country** from the drop-down menu.

– Check the **END USER LICENSE AGREEMENT (EULA)** and click **Save**.

e) **License Server**: Give the **License Server FQDN or IP address**, for example 127.0.0.2 and the **License Server Port**, for example 8080 and click **Save**.

f) **Features**: This setting allows you to activate some beta features and specifically:

- – Composer Automatic Software Updates
  – UC & Media Server Automatic Software Downloads
  – OSB & SBC Automatic Software Downloads
  – OSB & SBC Automatic Software Updates
  – OpenScape Voice Trace manager Automatic Software Downloads
  – OpenScape Contact Center Software Downloads
  – DLS Automatic Software Downloads
  – DLS Automatic Software Updates
  – Concierge Software Downloads
  – Xpressions Software Downloads
  – Upload Software bundle during Software Registration

– Multiple Communication Server Admin Software Downloads

Switch the slider(s) to ON and click **Save**.

NOTICE:

The OSV Automatic Software Downloads and Updates are active by default

3) Click **Download logs** to download the Composer logs as a zip file located under the path `/var/log/cmpnext`
4) Click **Update Composer**. This option appears only when you have enabled the feature **Composer Automatic Software Updates**.

   The **Update Composer** window appears. Select the **Repository** where you have stored manually the `.tar.gz` installation file and click **Update**.

   NOTICE:

   The repository in this case can only be a Hard Disk.
5) Click **About** to check your OpenScape Composer's version
6) Click **Logout** to exit the OpenScape Composer

4.2 Inventory

The OS Composer inventory consists of three different entities: Solutions, Hosts and Applications.

Supported Applications

The following Applications can be added to the OS Composer inventory:

- OpenScape Voice
- Open Scape Branch
- OpenScape Xpressions
- OpenScape Deployment Server
- OpenScape Unified Communications
- OpenScape Standalone Media Server
- OpenScape Contact Center Extensions, Concierge
- OpenScape Contact Center
- OpenScape Session Border Controller (For OSEE: OSSBC THIG).
- OpenScape Voice Trace Manager
- OpenScape Multiple Communication Server Admin

Every application needs an ssh account to give access to the OS Composer server. All applications except OpenScape Contact Center and OpenScape Contact Center Extensions, Concierge have ssh service pre installed. For OpenScape Contact Center and OpenScape Contact Center Extensions, Concierge you must manually install a program that provides ssh access.

NOTICE:

You can add DLS without an ssh access program installed, unless you want to use the backup/restore functionality. If so you need to install an ssh access program.

Initial Solution

The first time you want to create a solution

1) Click **+**
2) A new pop-up window **Create Solution** appears.
3) **Alias**: Fill in the alias of the solution, for example OpenScape Enterprise Express
4) **Description**: Provide a description
5) **Advanced Settings**: Fill in the solution's unique hash stored previously, to use any backup taken with a different Solution. You can find a list of all previously created solutions at `/opt/cmpnext/BACKUPS/solutionHistory.json`.
6) Click **Next**
7) Select **Application**. You can select from the list of section **Supported Applications**
8) Select **Host**: Click **Add new host..** and configure the following parameters for OSV:

   - Alias
   - FQDN or IP Address
   - srx Password

   or the following for any other application:

   - Alias
   - FQDN or IP Address
   - SSH Username
   - SSH Password
9) Click **Next**
10) The **Add Application** window appears. Configure the following parameters:

    - Alias
    - Security Policy
    - Ports
11) Click **Next**
12) A **Confirmation** window appears. Click **Finish** to finalize the solution.

4.2.1 Solution related actions

Solution is a group of related Hosts, where the OpenScape Applications are deployed.

You can perform the following actions in the Inventory page.

4.2.1.1 Add

1) Click the "**+**" to add applications to the Solution you have created. A pop-up window appears with all available applications:
   - OpenScape Voice
   - Xpressions
   - Deployment Server
   - OpenScape UC
   - Standard Media Server
   - Concierge
   - Contact Center
   - Session Border Controller
   - Trace Manager
   - Multiple Communication Server Admin

   NOTICE:

   When an OSV application is added, OS Composer automatically identifies and adds to the inventory the OSBs that are associated with the added OSV.

2) Once you select the application, select the host where the application is already deployed.

   NOTICE:

   To add a host using an FQDN, refer to chapter Host addition with Fully Qualified Domain Name (FQDN) for detailed instructions.You can select from the already created hosts or create a new one. For credentials, refer to chapter Default Application Passwords.

   NOTICE:

   For OSV applications and applications on an Integrated Simplex (UC and DLS), the Composer automatically creates the appropriate packet filter rule to communicate with the applications.

3) When you choose the host, a new **Add application** window pops up. In the **Alias** field, enter an alias name to your application.

   NOTICE: The configurable fields that appear in the **Add application** window depend on the selected host. For more information see also section **Edit** under Application related actions on page 26.

4) Click **Next** to view and confirm the details of the configuration settings before completing the process.
5) Click **Finish** to complete the process.

4.2.1.2 Refresh

OS Composer can be used by an operator to perform **Refresh** on one or many individual inventory items of an OpenScape Solution.Click the **Refresh** button to refresh all the applications you have in your Solution.

4.2.1.3 Check for Software Updates

OS Composer can be used by an operator to check for Software Updates. Click the "**...**" button and then click **Check for Updates** to perform the action. This option is only available when the SWS settings have been configured. See Configuring General Options.

4.2.1.4 Backup

OS Composer can be used to trigger a Backup for all the applications of the given Solution. OS Composer supports certain types of OpenScape applications such as OSV, DLS and others. For each of these, OS Composer knows what can be backed up and how this can be triggered using an interface of the corresponding solution element. When you backup a solution, all its applications are backed up.

The backup for UC & DLS applications in Integrated Simplex OSVs is included in the OSV backup.

How to Backup Solution

1) Click the "**...**" button
2) Click **Backup**

   A new pop-up window **Backup Solution <solution_name>** appears
3) Select the **Type of Backup** from the drop-down menu: You can select **Data** or **File-system**.

   NOTICE:

   Only OSV, UC and Standalone Media Server support file system backup. Therefore if a file system backup is initiated on a solution level, only these three applications will be backed up.
4) The **Location of Backup** is builtin by default
5) Click **Backup Now** to backup your solution.

4.2.1.5 Schedule Backup

When you want to backup on a later time

1) Click the "**...**" button
2) Click **Schedule Backup...**

   A new pop-up window **Schedules List for <solution_name> Solution** appears

3) Click **Add**
4) Select the **Type of Backup** from dropdown menu. The available values are:
   - Data
   - File-system
5) The **Location of Backup** is builtin by default.
6) Set the **Time** for the next Backup, within the day, and you can also set whether the backup will be repeated daily, weekly or monthly.
7) Click **Schedule Backup** to activate the scheduled backup.

> **NOTICE:** In case of the scheduled OSV Full system Backup, there must be a sufficient time-frame between the two nodes of the OSV cluster, as the backup of the second node starts only after the backup of the first node has been completed. The time frame differs from system to system. For more information regarding conflicts that might occur between jobs that have been scheduled or activated, see chapter Conflicts.

When you want to edit your scheduled backup:

1) Click the "**...**" button
2) Click **Schedule Backup...**

   A new pop-up window **Schedules List for <solution_name> Solution** appears
3) Click the edit icon  .
4) You can edit all parameters set in steps 4 - 6

When you want to delete a Scheduled Backup

1) Check the checkbox of the Scheduled Backup you want to delete. Click the **Delete Selected** button that appears to delete your selected Scheduled Backup(s).
2) Another way to delete a Scheduled Backup is to click the delete icon 

> **NOTICE:**
>
> DLS requires a disk partition in order to backup properly through OS Composer. Without this configuration, DLS backup fails with cause: *Error! failed to download from remote directory*

4.2.1.6 Repository Settings

To configure the backup locations:

1) Click the "**...**" button
2) Click **Repository Settings...**

   A new pop-up window **Repository Settings** appears. A list of all existing repositories appears, with builtin being the defualt one.

3) Click **Add**. A new pop-up window appears
   - Enter a **Name** for the new location.
   - Select a **Type**, either HD (Local Hard Disk), FTP or SFTP.
   - Give a **FQDN or IP Address**, for example example.com or 10.1.1.5
   - Select a **Port** from the numbers given
   - Give the **Repository Path**, for example (C:)
   - In the **Username** field, give the account name.
   - In the **Password** field, give the password of the account
   - Rewrite your password in the **Password (data encryption)** field, to encrypt it.
4) Select a repository and click **Edit** to configure it.
5) Select a repository and click **Delete** to delete it. You can use this action only when there are more than one existing repositories.
6) Select a repository and click **Set as default** to use it as the default location.

4.2.1.7 Display Notifications

You can choose whether you want see the notifications of the various applications or hide them through a drop-down menu.

1) Switch the slider to ON to display the notifications for all applications.
2) Switch the slider to OFF to hide the notifications for all applications.
3) Refresh your browser to activate the action.
4) You can choose to have some applications' notifications hidden and some displayed. Click the down-arrow to display the notifications from the application your want and hide the ones you don't want to see.
5) Refresh your browser to activate the action.

4.2.1.8 Restore

OS Composer can be used by an operator to restore data one or many applications (such as OSV, UC, Xpressions etc.) OS Composer supports only data restore, for file-system restore details, please see Manual File System Restore

How to Restore Solution

1) Click the "**...**" button
2) Click **Restore**

   A new pop-up window **Restore Solution** appears
3) Select the **Location of Backup** and the **Date/Time** it took place.
4) Click **Restore Backup**.

4.2.1.9 Delete

OS Composer can be used to remove a Solution from the Inventories.

How to Delete Solution

1) Click the "**...**" button

2) Click **Delete**

   A new pop-up window **Delete Solution** appears
3) Click **Delete** to permanently delete the solution or **Cancel** to abort

4.2.1.10 Manual File System Restore

Prerequisites

The hardware of the OS Composer computer system, to be restored, has not been damaged.

You backed up the file system of the relevant OS Composer computer system before the crash.

The backed up data is stored on an external computer system.

NOTICE:

The backed up data must have been stored on a hard disk formatted with ext2 or ext3. The free memory on the hard disk used must be three times larger than the backed up data.

The backed up data has not been damaged by the crash.

NOTICE:

When restoring data of installed components with data of different versions of the installed components, the restoration will not be performed. A corresponding error code is displayed. In this case, contact the next level of technical support

---

If you wish to restore the file system of an LVM-based OS Composer computer system: You have copied the restore script `lvRestoreUtility.sh` to the same location on the external computer system like the backed up data of the OS Composer Application computer system.

In case you wish to restore an LVM file system backup to a **new** hard disk, it is necessary, before executing `lvRestoreUtility.sh`, to create manually the partitions on the new disk, **exactly** as they were on the system, the backup was taken on. Especially the logical volumes on the new disk should have the same name and size.

After the restoration of the file system, the relevant OS Composer Application computer system is fully functional again and works with the configuration data existing when the file system backup was performed.

How to manually restore a OS Composer computer system after a system crash:

Step by Step

1) Insert the installation data carrier of the Linux operating system into the disk drive of the computer system you want to restore.

2) Reboot the computer system.

The computer system boots in the rescue mode.

3) Mount the data carrier on which the backup file of the file system is stored.

4) On the data carrier access the directory in which the backup file of the file system is stored.

5) How to restore the file system of a non-LVM-based OS Composer Application computer system:

a) Execute the following command to unzip the non-LVM-based restore script with its directory from the backup file:

`tar -xvf <`*backup file name*`> *Restore.sh`

b) Execute the following command to copy the unpacked non-LVM-based restore script to the current directory:

`cp <`*Osc-Install*[1]`>/servicetools/backup/Restore.sh .`

c) Execute the following command to start the non-LVM-based restore script:
`./Restore.sh`

The available archives are offered to you for selection.

d) Select the archive you wish to use for restoring.

e) Confirm your selection.

The restore process starts and information about the single Linux-based restore commands are put out via the shell.

If an error occurs while a Linux command is being executed, you can see this in the shell. Correct the error then as is described in the Linux product documentation.

6) If you wish to restore the file system of an LVM-based OS Composer Application computer system, execute the following command to start the LVM-based restore script:
`sh vlRestoreUtility.sh`

The restore process starts and information about the single Linux-based restore commands are put out via the shell.

If an error occurs while a Linux command is being executed, you can see this in the shell. Correct the error then as is described in the Linux product documentation.

7) Wait until the restore script used announces the end of the restoration.

8) Before starting OpenScape OS Composer Application, delete the contents of these two log files.

- `/var/siemens/common/log/osgi.log`
- `/var/siemens/common/log/osgi.err`

These files include the system start log information.

---

1 <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

9) Execute the following command on the computer system on which you have installed OpenScape OS Composer Application.
`/etc/init.d/symphoniad start`

OpenScape OS Composer Application starts. While the system starts, the system start log should not log any errors.

When the following message in the system startup log is displayed, all OpenScape OS Composer Application services have been started.
`******* Starting all instances done. *******`

Depending on the system configuration, it may take several minutes until all users configured in the system have been activated.

10) Execute the following command to put out the system startup log.
`tailf /var/siemens/common/log/osgi.log.`

11) Open the following error log file after the OpenScape OS Composer Application startup has finished.
`/var/siemens/common/log/osgi.err`

The error log file should not contain any error message.

12) The password for the **administrator@system** administrator account is after the data restoration reset to the value that was valid when the configuration files were backed up. If you want to reset the password of the **administrator@system** administrator account, execute the following command.

<*Osc-Install*[2]>`/servicetools/security/resetUserAccount.sh administrator@system` <*new password* >

You have now restored the OpenScape OS Composer Application computer system of Standard Duplex after a critical system crash.

4.2.2 Host related actions

4.2.2.1 Refresh

You can use the OpenScape Composer to **Refresh** the status of applications, whether their processes are running or not. To do so, click the **Refresh** button of the Application in order to also refresh the host that the application is deployed on. The status icon of the host indicates the SSH connectivity status.

4.2.2.2 Edit

OS Composer can be used by an operator to **Edit** one or more hosts of an OpenScape Solution.

How to edit hosts

1) Click the "**...**" button.

[2] <*Osc-Install* > is the setup directory of the OpenScape system:

`/opt/siemens/` respectively `/enterprise/`

2) Click **Edit**.

   A new pop-up window **Edit Host <host_name>** appears with a list of parameters for editing.

   - Alias
   - FQDN or IP Address
   - SSH Username
   - SSH Password

   For credentials, refer to chapter Default Application Passwords

3) Click **Save**.

4.2.3 Application related actions

In this section you can find information regarding all application related actions.

4.2.3.1 Refresh

The refresh action checks the application status and retrieves the application's current version. Click the **Refresh** button in order to perform this operation.

The status icon of the application indicates whether the application service is running or not.

- **Multi-node applications (OSV, DLS, SBC)**: You can the check the application service status for each node by hovering over the status icon
- **OSB**: You can check both the SSH connectivity to the host and the status of the application service by hovering over the status icon

---

NOTICE:

The XPR application is comprised of several different components, each with a different version. You can see the components' versions by clicking the 'View Components' button.

4.2.3.2 Synchronize

The Synchronize button retrieves the list of OSBs being configured in the OSV. This way you don’t have to add them manually, one-by-one. On the application you want to synchronize:

1) Click "**...**"
2) Click **Synchronize**.

4.2.3.3 Edit

Use the OS Composer to edit one or more applications of an OpenScape Solution. On the application you want to edit:

1) Click "**...**".
2) Click **Edit**.

3) A new window **Edit Application <application_name>** pops-up.
4) In the **Alias** field, give a new name for the application.
5) **Security Policy**: This parameter is applicable only for OSV. Select a value from the drop-down menu. The available values are:
   - NON_TLS
   - TLS
6) **Ports**: Select a value from the drop-down menu.
7) **Read community string**: This parameter is applicable only for OSV. Enter the read SNMP community string that corresponds to the application's side configuration.
8) Click **Save**.

4.2.3.4 Backup

Use the OS Composer to backup one or more hosts of an OpenScape Solution. The Backup operation is not enabled for UC applications on Integrated Simplex OSVs. The backup taken by the OSV includes all necessary data. The Backup operation for DLS applications on Integrated Simplex OSVs requires elevated privileges, for example the root user configured in the application's host. However, this is not required since the backup taken by the OSV also includes all necessary data.

On the application you want to backup:

1) Click the "**...**" button
2) Click **Backup**

   A new pop-up window **Backup <application_name>** appears
3) Select the **Type of Backup** from the dropdown menu. The available values are:
   - Data
   - File-system
4) Select the **Location of Backup** from the dropdown menu.The default value is builtin
5) Click **Backup Now** to backup your solution.

NOTICE:

The default backup type is **Local** and if no other path has been appointed, then the backup path is `/opt/cmpnext/BACKUPS`.

4.2.3.5 Schedule Backup

Use the OS Composer to schedule a backup of one or more applications of an OpenScape Solution. For the application you want to backup:

1) Click the "**...**" button
2) Click **Schedule Backup...**

   A new pop-up window **Schedules List for <application_name> Application** appears

3) Click **Add**

   A new pop-up window **Schedule Application Backup for <application_name>** appears
4) Select the **Type of Backup** from dropdown menu. The available values are:
   - Data
   - File-system
5) The **Location of Backup** is builtin by default.
6) Set the **Time** for the next Backup, within the day, and you can also set whether the backup will be repeated daily, weekly or monthly.
7) Click **Schedule Backup** to activate the scheduled backup.

When you want to edit your scheduled backup:

1) Click the "**...**" button
2) Click **Schedule Backup...**

   A new pop-up window **Schedules List for <application_name> Application** appears
3) Click the edit icon  .
4) You can edit all parameters set in steps 4 - 6

When you want to delete a Scheduled Backup

1) Check the checkbox of the Scheduled Backup you want to delete. Click the **Delete Selected** button that appears to delete your selected Scheduled Backup(s).
2) Another way to delete a Scheduled Backup is to click the delete icon  .

4.2.3.6 Restore

Use the OS Composer to restore one or more applications of an OpenScape Solution. For the application you want to restore:

1) Click the "**...**" button
2) Click **Restore**

   A new pop-up window **Restore <application_name>** appears
3) Select the **Location of Backup** and the **Date/Time** it took place.
4) Click **Restore Backup**.

4.2.3.7 File System Archives

File System backup is supported only for OSV & UC. This is actually an Image of the Hard-Disk. A Backup of this type is triggered only from the UI.

1) Click the "**...**" button
2) Click **File System Archives**

   A new pop-up window **File System archives <application_name>** appears
3) Select the **Location of Backup** from the dropdown menu.
4) Click **Backup Now** to backup your application.

4.2.3.8 Software Updates

Software downloads are supported for OSV, OSB, SBC, UC, Media Server and OSV Trace Manager and software updates for OSV, OSB, SBC and DLS.

NOTICE: You can make a Bulk Software Update for OSB and SBC. An  indication will notify you about available software updates.

---

1) Click the "**...**" button
2) Click **Schedule...** or **Now...** to proceed with the Software updates.

For detailed information, see chapter Software Updates

4.2.3.9 Check Application Health

This option is applicable only for OSV and performs a Rapidstat check and should be performed before running an update.

1) Click the "**...**" button
2) Click **Check Application Health**

4.2.3.10 Delete

Use the OpenScape Composer to delete one or more applications from the Inventory of OS Composer, not from the host. On the application you want to delete:

1) Click "**...**"
2) Click **Delete**.
3) A new window **Delete Application?** pops-up.
4) It requests confirmation for deleting the application.
5) Click **Delete**.

4.3 Software Updates

Software downloads are supported for all applications and software updates for OSV, OSB, SBC and DLS. This is a non-configurable option; it's purpose is to show, with an exclamation mark, that there are software updates available for the above applications.

Automatic downloads for Application from SWS will be stored under <repository_path>/downloads/<Application_Type>/<Version>

4.3.1 Register Software Bundles

You can register downloaded software bundles to make them available as target versions in the System Management's Software Updates. Here you can see all

registered software bundles. In case there is no connection with SWS, you have to manually store the files in your preferred repository.

4.3.1.1 Register OSV Software Bundles

You can register an OSV software bundle as described below:

Step by Step

1) Navigate to **System Management** > **Software Updates**.
2) Click **+**

   A new pop-up window **Application Type Selection** appears.
3) Select **OpenScape Voice**. The window changes to **Register OpenScape Voice Software Bundles**. Here you can register downloaded software bundles to make them available as target versions in the applications' Software Updates.
4) **Repository**: The location where the installation or software bundle files, such as zip or iso files, will be stored. Here you can select all kinds of repositories from the drop-down list, for example Hard Disks, ftp etc
5) **Metadata file**: Click **Browse** and locate the .json file of the software bundle that you have downloaded from SWS. Below is a Software Bundle Metadata template for OSV:

```
{
"description": "OpenScape Voice Server Software Part
 Number: A9Q00009232-1-50M3",
"JiTCOnly": "false",
"productType": "OpenScape Voice Server",
"version": "V10 R0.4.2 Patchsets",
"status": "eeQA - Pilot Usage",
"files": [
{ "filename": "c-V9R4.45.3.zip",
"checksum": "edba0a06696cab0bd3897aedfbcccb57",
"checksumAlgorithm": "MD5SUM",
"size": "80652721"
}
]
}
```

NOTICE:

a) a) The productType must be "OpenScape Voice Server"
b) b) The version must be of the format "<version> Images" for image software bundles and "<version> Patchsets" for patchset software bundles
c) c) All .zip or .iso files from the software bundle must be listed in the "files" tag with the correct filename, checksum, checksumAlgorithm and size.

---

6) **OSV Toolkit Metadata file**: Click **Browse** and locate the .json file of the OSV Toolkit software bundle that you have downloaded from SW. Make sure that you are registering the latest version You must register a toolkit to

perform a OSV Live Software Update. Below is a Software Bundle Metadata template for OSV Toolkit:

```
{
"description": "OpenScape Voice Server Software Part
 Number: P30152-P1367-B17-67-50M3",
"JiTCOnly": "false",
"productType": "OpenScape Voice Toolkit",
"version": "V1R9.68.0",
"status": "eeQA - Pilot Usage",
"files": [
{
"filename": "UNSPmigration-1.09-66.x86_64.rpm",
"checksum": "9258f2187f75bf2f2ce564c5cf7143e8",
"checksumAlgorithm": "MD5SUM",
"size": "1146776"
}
]
}
```

NOTICE:

a) a) The productType must be "OpenScape Voice Toolkit"

b) b) The .rpm file from the software bundle must be listed in the "files" tag with the correct filename, checksum, checksumAlgorithm and size.

7) **Software bundle file (Optional)**: Click **Browse** and locate the installation file that you have downloaded from SWS. This can either be a .zip or .iso file.

NOTICE:

Enable **Upload Software bundle during Software Registration** from the **Features** setting, as described in Configuring General Options.

You can either upload the installation file here or directly to the repository. For large files (for example the .iso file used for the Live Upgrade), you must upload the file directly to the repository and leave this field blank.

8) Click **Register**.

9) Click Back to return to the **Application Type Selection** window.

NOTICE:

To perform a Live Update you must register files for both OSV Server and Toolkit. The OSV Toolkit is not required for Rolling Upgrades.

4.3.1.2 Register OSB/SBC Software Bundles

You can register an OSB/SBC software bundle as described below:

Step by Step

1) Navigate to **System Management** > **Software Updates**.
2) Click **+**

   A new pop-up window **Application Type Selection** appears.
3) Select **OpenScape SBC** or **OpenScape Branch**. The window changes to **Register OpenScape SBC/ Branch Software Bundles**. Here you can register downloaded software bundles to make them available as target versions in the applications' Software Updates.
4) **Repository**: The location where the installation or software bundle files, such as zip or iso files, will be stored. Here you can select all kinds of repositories from the drop-down list, for example Hard Disks, ftp etc.
5) **Metadata file**: Click **Browse** and locate the .json file of the software bundle that you have downloaded from SWS. Below is a Software Bundle Metadata template for OSB:

```
{
"description": "",
"JiTCOnly": "false",
"productType": "OpenScape Branch",
"version": "V10 R0.4.0",
"status": "eeQA - Pilot Usage",
"files": [
{
"filename": "OSB-10.00.04.00-1.zip",
"checksum": "de3f89155afe1e1d05e2ca3a15aed352",
"checksumAlgorithm": "MD5SUM",
"size": "725104386"
}
]
}
```

NOTICE:

a) a) The productType should be "OpenScape Branch"
b) b) The .zip with pattern "OSB-*.zip" should be listed in the "files" tag with the correct filename, checksum, checksumAlgorithm and size.

Below is a Software Bundle Metadata template for SBC:

```
{
"description": "",
"JiTCOnly": "false",
"productType": "OpenScape SBC",
"version": "V10 R0.4.0",
"status": "eeQA - Pilot Usage",
"files": [
{
```

```
"filename": "oss-10.00.04.00-2.zip",
"checksum": "40bcd65c3069f82f2ed0fb8b11590872",
"checksumAlgorithm": "MD5SUM",
"size": "712491464"
}
]
}
```

NOTICE:

a) a) The productType should be "OpenScape SBC"

b) b) The .zip with pattern "oss-*.zip" should be listed in the "files" tag with the correct filename, checksum, checksumAlgorithm and size.

6) **Software bundle file (Optional)**: Click **Browse** and locate the installation file that you have downloaded from SWS. This can either be a .zip or .iso file.

NOTICE:

Enable **Upload Software bundle during Software Registration** from the **Features** setting, as described in Configuring General Options.

You can either upload the installation file here or directly to the repository. For large files, you must upload the file directly to the repository and leave this field blank.

7) Click **Register**.

4.3.1.3 Register DLS Software Bundles

You can register a DLS software bundle as described below:

Step by Step

1) Navigate to **System Management** > **Software Updates**.
2) Click **+**

   A new pop-up window **Application Type Selection** appears.
3) Select **Deployment Service**. The window changes to **Register Deployment Service Software Bundles**. Here you can register downloaded software bundles to make them available as target versions in the applications' Software Updates.
4) **Repository**: The location where the installation or software bundle files, such as zip or iso files, will be stored. Here you can select all kinds of repositories from the drop-down list, for example Hard Disks, ftp etc.
5) **Metadata file**: Click **Browse** and locate the .json file of the software bundle that you have downloaded from SWS. Below is a Software Bundle Metadata template for DLS:

```
{
"description": "Deployment Service",
```

```
"JiTCOnly": false,
"productType": "Deployment Service",
"version": "V10 R0.13.1",
"status": "eeQA - Pilot Usage",
"files": [
{
"filename": "dls_612.01_multinode.zip",
"checksum": "c3c25bda433327a8616786367c279037",
"checksumAlgorithm": "MD5SUM",
"size": "563746005"    },
{
"filename": "dls_612.01_singlenode.zip",
"checksum": "a7df9fb9db19c52558e36ae576567d67",
"checksumAlgorithm": "MD5SUM",
"size": "663097040"
}
]
}
```

NOTICE:

a) a) The productType must be "Deployment Service"

b) b) All .zip files from the software bundle must be listed in the "files" tag with the correct filename, checksum, checksumAlgorithm and size.

6) **Software bundle file (Optional)**: Click **Browse** and locate the installation file that you have downloaded from SWS. This can either be a .zip or .iso file.

NOTICE:

Enable **Upload Software bundle during Software Registration** from the **Features** setting, as described in Configuring General Options.

You can either upload the installation file here or directly to the repository. For large files, you must upload the file directly to the repository and leave this field blank.

7) Click **Register**.

8) Click Back to return to the **Application Type Selection** window.

4.3.2 Unregister Software Bundles

You can unregister software bundles so they are no longer available as target versions in the corresponding applications' Software Updates.

Unregistering a software bundle does not remove it from the file system.

Step by Step

1) Select the software bundle(s) you want to delete and click **Delete Selected** or click the delete icon  to the right of an individual bundle.

2) On the **Delete selected software update bundles?** window that pops-up, click **Delete**.

4.3.3 Bulk Software Updates

You can make a bulk software update for your OSB or SBC applications.

In the **Inventory** tab, click on the **...** button to display the options menu. There you can select the Bulk Software Updates option that you prefer. You can click on **Schedule...** to set the update to a specific time and date in the future, or click **Now...** to proceed with the bulk update immediately.

Schedule Update

If you select **Scedule...** a new screen pops up, with the following settings:

- **Application Type**

  Choose the application type that will be updated: e.g. OpeScape Branch, OpenScape SBC, etc.
- **Date**

  Date in the form of *dd/mm/yyyy*.
- **Time**

  Pick the specific time that the update will take place.
- **Repository**

  Select the repository to be used.
- **Target Version**

  Select one of the available versions.
- **Applications**

  Select one ore more applications from the available options according to the Application Type that you have selected.

Click on **Schedule Bulk Update** to proceed with the scheduling process and in the next screen read and confirm the user notice. Once you click on Confirm, the scheduled Bulk Update should be displayed under the Bulk Updates Schedules List for your solution. From here you can edit the existing scheduled update or add a new scheduled one.

Update Now

If you select **Now...** a new screen pops up, with the following settings:

- **Application Type**

  Choose the application type that will be updated: e.g. OpeScape Branch, OpenScape SBC, etc.
- **Repository**

  Select the repository to be used.
- **Target Version**

  Select one of the available versions.
- **Applications**

  Select one ore more applications from the available options according to the Application Type that you have selected.

Click on **Bulk Update** to proceed with the updating process and in the next screen read and confirm the user notice. Once you click on **Confirm**, the Bulk Update starts running.

When a Bulk Update is completed you will receive an email informing you about the successful procedure.

A cleanup files option is also available , when selecting **Yes** the software bundles will be deleted from the Repository.

4.4 Licenses

OS Composer is able to interface with a CLA (License Agent) and to provide information about activated license features.

License list

The License list dialog is displayed showing a list of licenses configured on the system. For each License, information regarding the Application, Feature, Licenses number, Expiration, Grace Period, Redundant, Status and the SIEL-ID is provided in that list.

- **Application**: The application for which the license is applicable
- **Feature**: Features allowed by the license file
- **Licenses**: Number of licenses left out of number bought
- **Expires**: The date the license expires
- **Grace Period**: Period of time, after the expiration of the license, during which you can still use the feature.
- **Redundant**: States whether the license is redundant or no.
- **Status**: The license status
- **SIEL-ID**: A contract number, necessary for maintenance operation

4.5 Software Subscription

This tab displays information about subscription license usage that is acquired via CMP. You can enable or hide this feature tab via **Settings** > **Features** by toggling the Software Subscription Licenses flag. It will only be displayed if Composer has collected any Software Subscription license reports from CMP.

The Subscription licenses list dialog is displayed showing the Subscription License report of the selected month. The current month is selected by default.

For each entry the following information is available:

- Node Name
- Node Type
- License Type
- Quantity
- Product ID
- Remaining Days
- Collection Error
- Last Collection Date

This list is updated on a daily basis, at 2am. The time is configurable in the `application-production.yml`. For more information on how to override

the OS Composer default configuration, check Overwriting the OS Composer default configuration on page 58.

Clicking on the refresh button will automatically sync information with CMP. After every sync, Composer consumes the corresponding Software Subscription licenses from the Licensing Server configured. Please refer to section Configuring General Options on page 15 for more information on how to configure the Licensing Server.

CMP SSL Server Settings

Navigate to **Settings** > **CMP SSL Server**.

> **NOTICE:** To show the CMP SSL Licenses Settings tab, the feature flag needs to be enabled

The following options are available:

- Use CMP Server (UC or MCSA) from inventory: Toggle this option between on and off to use CMP Server inventory. Enabling this option will result in the rest of the CMP SSL Server settings getting disabled and grayed out.

  When the aforementioned option is disabled then you need to manually configure the following SSL Server settings:
- CMP SSL Server FQDN or IP address: The server or IP that will be used.
- CMP SSL Server username: The user credentials for the CMP SSL server.
- CMP SSL Server password: The password for the CMP SSL server.

Click on **Apply and test connection** to test if you have entered the correct input in the server settings fields and apply the CMP SSL Server. In case that the server's connection fails, you will receive a message notifying you the failed connection.

Click **Save** to apply your changes. Now the selected SSL Server's licenses should be displayed on the **Software Subscription** tab upon hitting refresh.

4.6 Certificates

OS Composer is able to provide information about certificates. This can be done from the UI or manually

From the UI:

Please refer to How to deploy Custom Certificates on page 38 .

Manually:

The Certificates list dialog is displayed showing a list of certificates per application installed on the system. For each Application information regarding the certificate's Interface, Subject, Validation period and the issuer is provided in that list.

Next to each certificate there's a status icon indicating if the certificate is active ( ), expiring soon ( ) or already expired ( ).

- **Interface**: The interface for the certificate (e.g. HTTPS, SOAP) and port when applicable.

- **Subject**: The subject of the certificate.
- **Valid From**: Date and time from which the certificate is valid.
- **Valid To**: The date the certificate expires.
- **Issuer**: The issuer of the certificate.

4.6.1 How to change the ports of a Certificate

You are able to change the configured ports for your certificates.

Follow the steps below to change manually the port where the Composer will be looking for a certificate.

Step by Step

1) Open `/opt/cmpnext/app/certificatePorts.properties`:
`cd /opt/cmpnext/app/certificatePorts.properties`

2) Change manually the port you want to edit.
e.g.:
`PORT_CMP = 443`

3) Save the file.

4) Restart the server.
`service cmpn restart`

NOTICE: Changes will be reset when Composer is updated.

4.6.2 How to deploy Custom Certificates

Using Composer you can upload custom certificates for the applications for the OpenScape Solution. Currently the following are supported:

- OSV
  - Server Certificate (i.e. `server.pem`)
  - Client Certificate (i.e. `client.pem`)
- UC

NOTICE: Composer requires root access to deploy the interfaces on the list below. If any of the following interfaces is hosted on an Integrated Simplex, ensure that SSH root access has been given.

  - OSV Assistant SOAP Client
  - CMP Server Certificate
  - SPML Responder
  - Web Client
  - Apache2 WebServer
  - Media Server Interface
  - Media Server Secure Connection

- Composer
  - HTTPS interface certificate
- SBC and OSB

  (only supported for SBC/OSB with version V10 R2.1.0 and above)
  - Server certificate
  - SIP-TLS certificate
- SBC

  (interfaces supported for SBC only with version V10 R2.1.0 and above)
  - Android Push
  - iOS Push

It is assumed that the certificates have already been created and are ready to be uploaded.

Follow the steps below to deploy a custom certificate for an application.

Step by Step

1) In OpenScape Composer navigate to the **Certificates** tab.

2) Click on the options menu icon of the application you want to deploy the custom certificates to and click **Deploy custom certificates**.

3) In the Deploy custom certificates pop-up window of your selected application configure the available options for your specific certificate

The available options will be different according to the type of your selected application. Every certificate interface has different options or fields to be configured. For example not all interfaces have the Certificate file name field

or an **Import CA into truststore** section. In the list below, you can find some of the available options:

- **Interface type**:

  The interface we want to configure
- **Configure certificate**
  - **Certificate file name**:

    The name of the certificate file to be deployed (if none provided, will use the name of the uploaded file).
  - **Profile name**:

    The certificate profile name.
  - **Key**:

    The key file of the deployed certificate.
  - **Certificate**:

    The certificate to be deployed.
  - **CA certificate**:

    The CA certificate that has signed the certificate.
  - **Keystore password**
- **Import CA in truststore**
  - **CA certificate alias**:

    The certificate's alias (if none provided, a default value will be used).

    NOTICE: The alias needs to be unique in the truststore.
  - **CA certificate**:

    The CA certificate to be imported in the truststore
- **Restart services**:

  Whether to restart the services. e.g. for UC, symphonia will be restarted.

For more information, please refer to the *Certificate Management and Transport Layer Security(TLS)* Guide.

4) Configure the custom certificate settings and click **Browse** to select the certificate's file.

5) Click **Save** to load the custom certificate to your application.

6) Refresh the Certificates page to see your changes.

4.7 Notifications

The various OpenScape system components create Notifications that are displayed in the Notifications section.

Notifications list

The Notifications list dialog is displayed showing a list of notifications generated from the system. For each notification, information regarding its Severity, Type, Acknowledged Status, Date and a Message is provided in that list.

- **Severity**: The nature of the notification. Select a value from the drop-down menu: *Trace*, *Info*, *Warning* or *Error*
- **Type**: The type of the notification. Select a value from the drop-down menu
- **Acknowledged**: Whether the notification has been read by the administrator. Select from the drop-down menu: *false* or *true*
- **Timestamp**: The time period the notification was created. Give a date *from* and/or *to*
- **Message**: The information given by the notification.

5 Software Updates Actions

Software downloads are supported for all applications and software updates for OSV, OSB and SBC. This is a non-configurable option; it's purpose is to show, with an exclamation mark, that there are software updates available for the above applications.

5.1 OSV Software Updates

5.1.1 Schedule Software Updates

Use this option to schedule when to download or update to the desired OSV version.

1) Click the "**...**" button
2) Click **Schedule**

   A new pop-up window **Schedules List for <application_name> Application** appears. Only one schedule per type is possible.
3) Click **Add**

   A new pop-up window **Application Software Download for <application_name>** appears.
4) **Job Type**: There are two available values for this parameter:

   - Download (default). Select this value to download the desired OSV version
   - Update. Select this value to update your OSV version

   NOTICE:

   When you select this value, the name of the pop-up window changes to **Application Software Update for <application_name>**

   ---
5) **Software Update Type**: This parameter appears only when you have selected the value "Update" in the **Job Type** parameter. There are two available values for this parameter:

   - Live Update: See Live Update
   - Rolling Upgrade: See Rolling Upgrade
6) **Repository**: The location where the software will be stored. The default value is builtin
7) **Target Versions**: This parameter allows you to choose the OSV version you want to download or update.

   - When you have selected "Download" as **Job Type**, you must select at least one target version either from Images or Emergency Patchsets
   - When you have selected "Update" as **Job Type** and Live Update as **Software Update Type**, you must select an image, and optionally a patchset. When the image you have selected is OSV's current image, the patchset is required. When you have selected Rolling Upgrade as **Software Update Type**, you must select one patchset.
8) **Date**: Set the desired date for the download/update

9) **Time**: Set the desired time for the download/update
10) **Cleanup installation files from repository after successful update**: Click **Yes** or **No**. This parameter appears only when you have selected "Update" as **Job Type** and is a mandatory one.
11) **Check application's health status**: This parameter appears only when you have selected Update as **Job Type** and is a mandatory one.
    - Click **Yes**. Check is executed automatically during the update.
    - Click **No**. Run manually the application's health status as described in Check Application Health
12) **License Settings**: This parameter appears only when you have selected:
    - **Job Type**: Update
    - **Software Update Type**: Live Update

    When performing a major version upgrade, you can upload the license files to activate them. When the OSV is a cluster, you can upload the license files for both nodes, whereas for a simplex OSV, you can upload the license file for the UC applications as well.

    Select the appropriate `.lic` file you have stored locally. The licenses can be uploaded after the update.
13) **Synchronize the partitions before Rolling Upgrade**: This parameter appears only when you have selected:
    - **Job Type**: Update
    - **Software Update Type**: Rolling Upgrade

    You have the following options:
    - **Yes**: This option executes the `sync8K` command
    - **No**: The command will not be executed
14) Click **Schedule Download/Update**
15) The **Schedules List for <host_name> Application** has now the created task. You can have one Download scheduled task and one Update task.
16) Click the edit icon  to configure the parameters of the scheduled task.

    NOTICE:

    You can't edit the **Job Type** parameter or the licenses files uploaded. To change them you must delete the schedule and create a new one.
17) Select the scheduled task and click **Delete Selected** or click the delete icon  to delete your scheduled task.

5.1.2 Software Updates Now

Use this option to download or update the OSV version you are currently running.

1) Click the "**...**" button
2) Click **Now**

   A new pop-up window **Application Software Download for <application_name>** appears.

3) **Job Type**: There are two available values for this parameter:
   - Download (default). Select this value to download the desired OSV version
   - Update. Select this value to update your OSV version

   NOTICE:

   When you select this value, the name of the pop-up window changes to **Application Software Update for <application_name>**

   ---

4) **Software Update Type**: This parameter appears only when you have selected the value "Update" in the **Job Type** parameter. There are two available values for this parameter:
   - Live Update: See Live Update
   - Rolling Upgrade: See Rolling Upgrade
5) **Repository**: The location where the software will be stored. The default value is builtin
6) **Target Versions**: This parameter allows you to choose the OSV version you want to download or update.
   - When you have selected Download as **Job Type**, you must select at least one target version either from Images or Emergency Patchsets
   - When you have selected "Update" as **Job Type** and Live Update as **Software Update Type**, you must select an image, and optionally a patchset. When the image you have selected is OSV's current image, the patchset is required. When you have selected Rolling Upgrade as **Software Update Type**, you must select one patchset.
7) **Cleanup installation files from repository after successful update**: Click **Yes** or **No**. This parameter appears only when you have selected Update as **Job Type** and is a mandatory one.
8) **Check application's health status**: This parameter appears only when you have selected Update as **Job Type** and is a mandatory one.
   - Click **Yes**. Check is executed automatically during the update.
   - Click **No**. Run manually the application's health status as described in Check Application Health
9) **License Settings**: This parameter appears only when you have selected:
   - **Job Type**: Update
   - **Software Update Type**: Live Update

   When performing a major version upgrade, you can upload the license files to activate them. When the OSV is a cluster, you can upload the license files for both nodes, whereas for a simplex OSV, you can upload the license file for the UC applications as well.

   Select the appropriate `.lic` file you have stored locally. The licenses can be uploaded after the update.

10) **Synchronize the partitions before Rolling Upgrade**: This parameter appears only when you have selected:

    - **Job Type**: Update
    - **Software Update Type**: Rolling Upgrade

    You have the following options:

    - **Yes**: This option executes the `sync8K` command
    - **No**: The command will not be executed

5.1.3 Live Update

This feature allows you to schedule or perform an update of the OSV image. Before starting a live update, perform the following checks:

1) Ensure the `/repository/update` directory has **sym:rtpgrp** ownership. When this is not the case, execute, as the root user, the following command:

   ```
   chown sym:rtpgrp /repository/upload/
   ```

   IMPORTANT:

   Execute the command on both nodes of a Duplex OSV deployment

2) For an OSV on virtual machines only:

   - Ensure that no drives are mounted on any node of the OSV.
   - Ensure that the `/etc/fstab` file permissions are: **- rw--r--r**

     When the permissions are different than the ones indicated above, change the file permissions, as a root user, with the following command:

     ```
     chmod a+r /etc/fstab
     ```

     IMPORTANT:

     Execute the command on both nodes of a virtual Duplex OSV deployment

3) When the OSV version is smaller than V9R4.41.0, check the manual actions that are required for the update in the release notes.

5.1.4 Rolling Upgrade

Use this feature when you want to install a patchset in a current image. When you select "Rolling Upgrade" as a **Software Update Type**, the Images and Licenses do not appear as available options.

5.2 OSB/SBC Software Updates

5.2.1 Schedule Software Updates

Use this option to schedule when to download or update the desired OSB/SBC version.

1) Click the "**...**" button
2) Click **Schedule**

   A new pop-up window **Schedules List for <application_name> Application** appears. Only one schedule per type is possible.
3) Click **Add**

   A new pop-up window **Application Software Download for <application_name>** appears.
4) **Job Type**: There are two available values for this parameter:
   - Download (default). Select this value to download the desired OSB/SBC version
   - Update. Select this value to update your OSB/SBC version

   ---

   NOTICE:

   When you select this value, the name of the pop-up window changes to **Application Software Update for <application_name>**

   ---
5) **Repository**: The location where the software will be stored. The default value is builtin
6) **Target Versions**: This parameter allows you to choose the OSB/SBC version you want to download or update.
   - When you have selected "Download" as **Job Type**, you must select at least one target version from the list.
   - When you have selected "Update" as **Job Type**, you must to select one target version from the list.
7) **Date**: Set the desired date for the download/update
8) **Time**: Set the desired time for the download/update
9) **Cleanup installation files from repository after successful update**: Click **Yes** or **No**. This parameter appears only when you have selected "Update" as **Job Type** and is a mandatory one.
10) Click **Schedule Download/Update**
11) The **Schedules List for <host_name> Application** has now the created task. You can have one Download scheduled task and one Update task.
12) Click the edit icon  to configure the parameters of the scheduled task.

    NOTICE:

    You can’t edit the **Job Type** parameter

    ---
13) Select the scheduled task and click **Delete Selected** or click the delete icon  to delete your scheduled task.

5.2.2 Software Updates Now

Use this option to download or update the OSB/SBC version you are currently running.

1) Click the "**...**" button
2) Click **Now**

   A new pop-up window **Application Software Download for <application_name>** appears.
3) **Job Type**: There are two available values for this parameter:
   - Download (default). Select this value to download the desired OSB/SBC version
   - Update. Select this value to update your OSB/SBC version

   NOTICE:

   When you select this value, the name of the pop-up window changes to **Application Software Update for <application_name>**
4) **Repository**: The location where the software will be stored. The default value is builtin
5) **Target Versions**: This parameter allows you to choose the OSB/SBC version you want to download or update.
   - When you have selected Download as **Job Type**, you must select at least one target version from the list
   - When you have selected Update as **Job Type**, you must to select one target version from the list.
6) **Cleanup installation files from repository after successful update**: Click **Yes** or **No**. This parameter appears only when you have selected Update as **Job Type** and is a mandatory one.

5.3 UC/ Media Server/ Multiple Communication Server Admin/ Xpressions/ Contact Center/ Concierge/ DLS Software Updates

This section describes how to configure software updates.

Clarification
Stand Alone MS Software update is not yet implemented in Composer

5.3.1 Schedule Software Updates

The Software Updates operations are not enabled for UC & DLS applications on Integrated Simplex OSVs. They are automatically updated during an OSV Live update.

Use this option to schedule when to download the desired UC/ Media Server/ Multiple Communication Server Admin/ Xpressions/ Contact Center/ Concierge/ DLS version.

1) Click the "**...**" button

2) Click **Schedule**

   A new pop-up window **Schedules List for <application_name> Application** appears. Only one schedule per type is possible.
3) Click **Add**

   A new pop-up window **Application Software Download for <application_name>** appears.
4) **Job Type**: There is one available value for this parameter:

   - Download (default). Select this value to download the desired version
5) **Repository**: The location where the software will be stored. The default value is builtin
6) **Target Versions**: This parameter allows you to choose the version you want to download.

   - Select at least one target version from the list
7) **Date**: Set the desired date for the download
8) **Time**: Set the desired time for the download
9) Click **Schedule Download**
10) The **Schedules List for <application_name> Application** has now the created task. You can have one Download scheduled task.
11) Click the edit icon to configure the parameters of the scheduled task.

    NOTICE:

    You can't edit the **Job Type** parameter
12) Select the scheduled task and click **Delete Selected** or click the delete icon to delete your scheduled task.

5.3.2 Software Updates Now

Use this option to download the UC/ Media Server/ Multiple Communication Server Admin/ Xpressions/ Contact Center/ Concierge/ DLS version you are currently running.

1) Click the "**...**" button
2) Click **Now**

   A new pop-up window **Application Software Download for <application_name>** appears.
3) **Job Type**: There is one available value for this parameter:

   - Download (default). Select this value to download the desired version
4) **Repository**: The location where the software will be stored. The default value is builtin
5) **Target Versions**: This parameter allows you to choose the version you want to download or update.

   - Select at least one target version
6) Click **Download**.

5.4 OpenScape Voice Trace Manager Server Software Updates

5.4.1 Schedule Software Updates

Use this option to schedule when to download the desired OSV Trace Manager version.

1) Click the "**...**" button
2) Click **Schedule**

   A new pop-up window **Schedules List for <application_name> Application** appears. Only one schedule per type is possible.
3) Click **Add**

   A new pop-up window **Application Software Download for <application_name>** appears.
4) **Job Type**: There is one available value for this parameter:
   - Download (default). Select this value to download the desired OSV Trace Manager Server version
5) **Repository**: The location where the software will be stored. The default value is builtin
6) **Target Versions**: This parameter allows you to choose the OSV Trace Manager version you want to download.
   - Select at least one target version from the list
7) **Date**: Set the desired date for the download
8) **Time**: Set the desired time for the download
9) Click **Schedule Download**
10) The **Schedules List for <application_name> Application** has now the created task. You can have one Download scheduled task.
11) Click the edit icon  to configure the parameters of the scheduled task.

    NOTICE:

    You can't edit the **Job Type** parameter
12) Select the scheduled task and click **Delete Selected** or click the delete icon  to delete your scheduled task.

5.4.2 Software Updates Now

Use this option to download the OSV Trace Manager version you are currently running.

1) Click the "**...**" button
2) Click **Now**

   A new pop-up window **Application Software Download for <application_name>** appears.
3) **Job Type**: There is one available value for this parameter:
   - Download (default). Select this value to download the desired OSV Trace Manager Server version

4) **Repository**: The location where the software will be stored. The default value is builtin
5) **Target Versions**: This parameter allows you to choose the OSV Trace Manager version you want to download or update.
   - Select at least one target version
6) Click **Download**.

5.5 Device Firmware Updates

You can download automatically firmware updates for your CP Phone device. Automatic downloads for DLS Devices firmware from SWS will be stored under <repository_path>.

5.5.1 Prerequisites

The following parameters must have been configured before proceeding to Device Firmware Update actions:

- FTP repository is configured on DLS side.
- The same repository of FTP type is configured on Composer and appears in the repositories under **Repository Settings**.
- You have checked for the latest software Updates:

  In the **Inventory** tab, click on the **...** button to display the options menu. Click **Check for Software Updates**.

  The **Device Firmware Updates** area is displayed after clicking the "**...**" button. You can either schedule a Device firmare download or perform it in real time.

5.5.2 Schedule Software Updates

Use this option to schedule when to download or update the desired Devices version.

1) Click the "**...**" button.
2) Click **Schedule**.

   A new pop-up window **Schedules List for <application_name> Application** appears. Only one schedule per type is possible.
3) Click **Add**.

   A new pop-up window **Application Software Download for <application_name>** appears.
4) **Job Type**: There are two available values for this parameter:
   - Download (default). Select this value to download the desired devices type version.
5) **Repository**: The location where the device software will be stored. The default value is builtin.

6) **Target Versions**: This parameter allows you to choose the devices type version you want to download or update.
   - When you have selected "Download" as **Job Type**, you must select at least one target version from the list.

   NOTICE: Composer downloads the device firmware and prompts the DLS to perform the update. The update option should be disabled for the devices formware on the Composer side.

7) **Date**: Set the desired date for the download/update.
8) **Time**: Set the desired time for the download/update.
9) Click **Schedule Download/Update**.
10) The **Schedules List for <host_name> Application** has now the created task. You can have one Download scheduled task and one Update task.
11) Click the edit icon  to configure the parameters of the scheduled task.

    NOTICE:

    You cannot edit the **Job Type** parameter.

12) Select the scheduled task and click **Delete Selected** or click the delete icon  to delete your scheduled task.

5.5.3 Software Updates in real time

Use this option to download the Devices version you are currently running.

1) Click the "**...**" button.
2) Click **Now**.

   A new pop-up window **Devices Firmware Download for <application_name>** appears.
3) **Job Type**:
   - Download (default). Select this value to download the desired devices version updates.

   NOTICE:

   There is no **Update** option. The firmware update is done automatically from DLS side.

4) **Repository**: The location where the software will be stored. The default value is builtin.

   NOTICE: It is recommended to select the repository that has been configured both on DLS and Composer so that the update process is done automatically.

5) **Device Type**: A list of device types that exist in the repository.
6) **Target Versions**: This parameter allows you to choose the device type version you want to download.

7) Click **Download** to initiate the download in case you have selected Download as **Job Type**.

NOTICE: Device types of the same version that belong in the same CP Phone family (e.g. CP400 SIP and CP600 SIP) share the same firmware. Therefore, if you have selected to download a version of e.g. CP400 SIP, the same version of CP600 does not appear anymore in the list in order to avoid downloading the same firmware twice.

---

6 Backups

6.1 Application Requirements for Composer Backups

Applications on Windows servers (Xpressions, Concierge, Contact Center, Deployment Service and Trace Manager)

The Composer can download the backup files generated by the application, only when OpenSSH is installed on the Windows server. When installed, you can connect via SSH to the application server using the credentials used to logon to the Windows server.

OpenScape UC & Media Server

To enable a File-System backup for the UC and Media Server applications, you must install the "dump rpm" on the server. For more information, check the application's Administrator Documentation.

6.2 How to take a backup manually

When the Composer fails to take a backup, you can manually take a backup as described below.

UC

1) Login to the Common Management Platform and navigate to **Maintenance** > **Recovery** > **Backup & Restore** > **Backup**
2) Select an archive and click **Next**.
3) Choose a backup type
4) Select **Application Server**
5) Click **Start**

Media Server

1) Login to the Media Server Common Management Platform and navigate to **Maintenance** > **Recovery** > **Backup & Restore** > **Backup**
2) Select an archive and click **Next**.
3) Choose a backup type
4) Select **Application Server**
5) Click **Start**

Multiple Communication Server Admin

1) Login to the MCSA Common Management Platform and navigate to **Maintenance** > **Recovery** > **Backup & Restore** > **Backup**
2) Select an archive and click **Next**.
3) Choose a backup type
4) Select **Application Server**
5) Click **Start**

OpenScape Voice

1) Login to the Common Management Platform that contains the OSV in its inventory. Navigate to **Maintenance** > **Recovery** > **Backup & Restore** > **Backup**
2) Select an archive and click **Next**.
3) Choose a backup type
4) Select the OSV server you want to backup
5) Click **Start**

Session Border Controller

1) Login to the OpenScape SBC Management Portal. Navigate to **Maintenance** > **Import & Export** > **Export**
2) Click **Export all**

OpenScape Branch

1) Login to the OpenScape Branch Management Portal. Navigate to **Maintenance** > **Import & Export** > **Export**
2) Click **Export all**

OpenScape Deployment Service

1) Open a cmd on the application server and execute the following command:

   ```
   C: && cd "C:\Program Files\DeploymentService\Tomcat
   \webapps\DeploymentService\database\" && dbexport.bat
   dlsDbExport.zip
   ```

2) The backup file's name is `dlsDbExport.zip` and you can find it in: `C:\Program Files\DeploymentService\Tomcat\webapps \DeploymentService\database\`

NOTICE:

`C:\Program Files\DeploymentService\` is the default installation path. When the Deployment Service is installed in a different path, replace the `C:\Program Files \DeploymentService\` part of the command with the actual installation path.

OpenScape Xpressions

1) Open a cmd on the application server and execute the following command:

   ```
   C: && cd "c:\openscape\xpr\bin" && "osee-backup.cmd"
   ```

2) The backup file's name is `osee.zip` and you can find it in: `c:\openscape \xpr\`

NOTICE:

`c:\openscape\xpr\` is the default installation path. When Xpressions is installed in a different path, replace the `c: \openscape\xpr\` part of the command with the actual installation path.

OpenScape Concierge

1) Open a cmd and execute the following command:

   ```
   C: && cd "C:\Program Files (x86)\OpenScape Contact
   Center Extensions\scripts" && BackupConcierge.cmd
   ```

2) You can find the backup file in: `C:\Program Files (x86)\OpenScape Contact Center Extensions\scripts\ConciergeBackup`

NOTICE:

`C:\Program Files (x86)\OpenScape Contact Center Extensions` is the default installation path. When Concierge is installed in a different path, replace the `C:\Program Files (x86)\OpenScape Contact Center Extensions` part of the command with the actual installation path.

OpenScape Contact Center

1) Open a cmd on the application server and execute the following command:

   ```
   C: && cd "C:\Program Files (x86)\OpenScape\Contact
   Center" && "FULLBACKUP.BAT"
   ```

2) The backup file's name is `vm_0_L0` and you can find it in: `C:\Program Files (x86)\OpenScape\Contact Center\Backups`

NOTICE:

`C:\Program Files (x86)\OpenScape\Contact Center` is the default installation path. When Contact Center is installed in a different path, replace the `C:\Program Files (x86)\OpenScape\Contact Center` part of the command with the actual installation path.

OpenScape Trace Manager

1) Open a cmd on the application server and execute the following command:

   ```
   C: && cd "C:\OSV-TM" && "OSVTMBackup.bat"
   ```

2) The backup file's name is `Backup.zip` and you can find it in: `C:\Tracedata\`

NOTICE:

`C:\OSV-TM` is the default installation path. When Trace Manager is installed in a different path, replace the `C:\OSV-TM` part of the command with the actual installation path.

6.3 Reusing Backups

Every solution created on the Composer, has an automatically generated unique hash. This hash is used for storing all backups taken by the Composer for that specific solution.

A new solution is not able to use the backups taken by an older solution, unless the new solution has been created with the older solution's unique-hash.

Specifically, when you want to create a Solution that will be able to use another Solution's backups (for example, because the old Solution got deleted), perform the following steps:

1) Store the old Solution's hash

The file `/opt/cmpnext/BACKUPS/solutionHistory.json` on the Composer server contains a list of all solutions created on the specific Composer and their unique hashes.

When the `solutionHistory.json` is not available, you can find the unique-hash on any of the repositories that contain Composer backups. The repository folder contains a "solutions" folder, which contains another folder and the name of the sub-folder is the solution's unique hash.

2) Add the solution using the unique hash

When adding the solution, click **Advanced Settings** and enter the Unique Hash

3) Add the applications you want to include in the solution

4) Add the repositories containing the backups

7 Start/Stop OpenScape Composer Server

Follow the instruction below to start or stop the OS Composer server.

Start the OS Composer Server

Follow the steps exactly as they are described below to start the OS Composer Server

1) Connect to the VM where OS Composer is hosted via SSH as root user.

   OS Composer is hosted on the same VM with UC
2) Execute the following script:

```
systemctl start cmpn
```

Stop the OS Composer Server

Follow the steps exactly as they are described below to stop the OS Composer Server.

1) Connect to the VM where OS Composer is hosted via SSH as root user.

   OS Composer is hosted on the same VM with UC
2) Execute the following script:

```
systemctl stop cmpn
```

8 Overwriting the OS Composer default configuration

You can configure the OS Composer partly through the Composer UI and partly through the command line interface.

The OS Composer default configuration is stored in the `application.yml` file. This file is overwritten during upgrades and you must not modify it. It is located under `/opt/cmpnext/app/` and is written in YAML syntax.

Apply any custom configuration to the file `application-production.yml`, which is located in the same folder as the `application.yml` and is also written in YAML syntax.

Below you can find some snippet examples to add to the `application-production.yml` file:

- Overwrite the default port of OS Composer Server

  `server.port: <CUSTOM_PORT>`
- Overwrite the default OS Composer Server certificate (The one presented on the Browser)

  `server.ssl.key-alias: <CUSTOM_CERTIFICATE_ALIAS>`
- Overwrite the default schedule of SWS check

  `sws.periodic.check.cron.expression: <CUSTOM_CRON_TIME>`
- Overwrite the default schedule of certificates check

  `cert.periodic.check.cron.expression: <CUSTOM_CRON_TIME>`
- Overwrite the default schedule of license check

  `license.periodic.check.cron.expression: <CUSTOM_CRON_TIME>`
- Overwrite the default schedule of software subscription license check

  `subscription.license.periodic.check.cron.expression: <CUSTOM_ CRON_TIME>`

9 Managing Certificates in OpenScape Composer

Follow the instructions below to manage certificates in OpenScape Composer.

Cerificate format

OS Composer uses two JKS formatted certificate repositories:

- **cmpKeyStore.jks**, used to store private keys and own identity certificates.
- **cmpTrustStore.jks**, used to store certificates from trusted Certificate Authorities.

NOTICE:

Both Keystore and Truststore are located under `/opt/cmpnext/app/`.

Purpose

The purpose of certificate management is to secure communication between:

- OS Composer and the Browser.
- OS Composer and the BE SOAP servers (OSV, DLS, etc.).

The default installation of OS Composer comes with one self-signed identity certificate, which is used from OS Composer as server certificate. Additionally, the default Certificate Authority certificate of OSV is by default installed in the Truststore.

NOTICE: Custom Certificate requirements are described in OpenScape Solution Set V10, Certificate Management and Transport Layer Security (TLS), Administrator Documentation, Issue 19 under Section 3.1.

9.1 How to add a certificate to the Keystore

Follow the steps below to add a custom certificate (PKCS#12) to the Keystore.

NOTICE: To avoid any errors, it is advised to copy the following commands in a notepad program and edit them accordingly before running them on the relevant command line.

IMPORTANT: The custom certificate used for Composer GUI should not have Client Authentication enabled in the Extended Key Usage, as it may cause conflicts with the SWS Client Certificate.

Step by Step

1) Change to the directory `/opt/cmpnext/app`:

```
cd /opt/cmpnext/app/
```

2) Add Java's keytool to the classpath:

```
export JAVA_HOME=/opt/cmpnext/packages/ibm-java-
x86_64-80/jre/
export PATH=$JAVA_HOME/bin:$PATH
```

3) Import the custom certificate to the keystore with a unique alias <UNIQUE_ALIAS>:

```
keytool \
-importkeystore \
-srckeystore <PKCS#12_FILE> \
-srcstorepass <PKCS#12_PASSWORD> \
-srcalias <PKCS#12_ALIAS> \
-srcstoretype PKCS12 \
-destkeystore cmpKeyStore.jks \
-deststorepass <KEYSTORE_PASSWORD> \
-deststoretype JKS \
-destalias <UNIQUE_ALIAS>
```

NOTICE:

In case there is a certificate with the same alias in the Keystore, the keytool prompts you to overwrite it or not. If you want to replace the existing certificate with the new one, select yes. Otherwise, import your certificate with another alias.

4) Add the <UNIQUE_ALIAS> in the appropriate `application-production.yml` file, as described in Overwriting the OS Composer default configuration on page 58 under **Overwrite the default OS Composer Server certificate** in order to edit the default configuration.

5) Change the custom certificate's private key password to be the same with the Keystore's one. The Keystore's password is stored in the 'server.ssl.key-store-password' key in `application.yml` or `application-production.yml` (for custom passwords) in the same directory.

```
keytool \
-keypasswd \
-alias <UNIQUE_ALIAS> \
-keypass <PKCS#12_PASSWORD> \
-new <KEYSTORE_PASSWORD> \
-keystore cmpKeyStore.jks \
-storepass <KEYSTORE_PASSWORD>
```

6) Restart the server.

```
service cmpn restart
```

9.2 How to customize the OS Composer server certificate

Follow the instructions below to customize the OpenScape Composer server certificate.

Customize via the UI:

To customize the OS Composer server certificate via the UI, refer to Section How to deploy Custom Certificates on page 38.

Customize manually:

The OS Composer uses by default, as server certificate, the certificate with alias "composerserver(default)", which is installed by the RPM.

To replace the OS Composer server certificate with a custom one:

Add a custom certificate to the Keystore, as described in Section How to add a certificate to the Keystore with a unique alias <SERVER_NEW_ALIAS>, which differs from the default 'composerserver(default).

9.3 How to add a certificate to the Truststore

Follow the steps below to add a custom certificate (PEM) to the Truststore.

Step by Step

1) Change to the directory `/opt/cmpnext/app/`:
```
cd /opt/cmpnext/app/
```
2) Add Java's keytool to the classpath:
```
export JAVA_HOME=/opt/cmpnext/packages/ibm-java-
x86_64-80/jre/
export PATH=$JAVA_HOME/bin:$PATH
```
3) Import the CA's certificate to the truststore:
```
keytool\
-importcert\
-file ${PEM_FILE}\
-alias "${PEM_CERT_ALIAS}"\
-keystore cmpTrustStore.jks \
-storepass <TRUSTSTORE_PASSWORD>
```
4) Restart the server:
```
service cmpn restart
```

NOTICE:

When there is already a certificate with the same alias in the Truststore, then use another alias or delete the existing one.

NOTICE:

The Truststore password is stored at the 'server.ssl.trust-store-password' key in `application.yml` in the same directory.

9.4 How to remove a Certificate from Keystore/Truststore

Follow the steps below to remove a certificate from the Keystore/Truststore.

NOTICE:

To avoid any errors, it is advised to copy the following commands in a notepad program and edit them accordingly before running them on the relevant command line.

Step by Step

1) Change to the directory `/opt/cmpnext/app/`:

```
cd /opt/cmpnext/app/
```

2) Add Java's keytool to the classpath:

```
export JAVA_HOME=/opt/cmpnext/packages/ibm-java-
x86_64-80/jre/
export PATH=$JAVA_HOME/bin:$PATH
```

3) List the existing aliases:

```
keytool -list -keystore
 {cmpKeyStore.jks,cmpTrustStore.jks} -v
```

4) From the existing aliases, find the alias of the certificate that you want to remove and remove it from the Keystore:

```
keytool -delete -alias <CERTIFICATES_ALIAS> -keystore
 {cmpKeyStore.jks,cmpTrustStore.jks}
```

NOTICE:

The certificate's private key password must be the same with the keystore's password.

5) Restart the server:

```
service cmpn restart
```

10 Conflicts

In some cases there can be a conflict between jobs you have scheduled or activated. These jobs are given in the following table

Job	Application Backup	Application File-System Backup	Application Restore	Solution Backup	Solution File-System Backup	Solution Restore	Download Software	Update Software	Bulk Software Updates
Synchronization	X	X	X	X	X	X	X	X	X
Application Backup	X	X	X	X	X	X	X	X	X
Application File-System Backup	X	X	X	X	X	X	X	X	X
Application Restore	X	X	X	X	X	X	X	X	X
Solution Backup	X	X	X	X	X	X	X	X	X
Solution File-System Backup	X	X	X	X	X	X	X	X	X
Solution Restore	X	X	X	X	X	X	X	X	X
Download Software							X		X
Update Software	X	X	X	X	X	X	X	X	X
Bulk Software Updates	X	X	X	X	X	X	X	X	X

Where X = Conflict

NOTICE:

When a job conflict occurs, a notification is created to report the job conflict. The notifications for jobs that will run again sometime in the future (for example, hourly, daily, weekly or monthly schedules) will not be shown in the inventory. All notifications can be found in the **Notifications** tab.