Chapter 8

Network Provisioning (CVP)

The Network Provisioning Screen presents a hierarchical view of the network configuration. It is not a network topology; it is a configuration tree view. To setup the network topology for Telemetry, see Device Management. The switches at the bottom of the tree inherit the configuration specified in the containers above them as well as the configuration that is specific to them. The containers and switches all have sub menus that are accessed by right mouse clicking on them. The main features of the screen are described below.

Note
Switches that have been added to the network from new will ZTP boot using generic details from CVP and appear in the Undefined container.

Sections in this chapter include:

- Network Provisioning View on page 164
- Container Level Actions (Create, Rename, Delete) on page 167
- Device Bootstrap Process on page 169
- Device Level Actions on page 170
- Replacing Switches Using the ZTR Feature on page 182
- Managing Configurations on page 184
- Configuration Validation on page 187
- Using Hashed Passwords for Configuration Tasks on page 188
- Reconciling Configuration Differences on page 188
- Managing EOS Images Applied to Devices on page 193
- Rolling Back Images and Configurations on page 195
- Device Labels on page 198
- Viewing Containers and Devices on page 202
- Device Compliance on page 204
- Notifications for Container-level Compliance Checks and Reconciles on page 209
- Global Search on page 210
- Management IP on page 214
8.1 Network Provisioning View

The topology view of the Network Provisioning screen is a tree structure that consists of containers and devices. This view represents the current groupings of devices (devices grouped by container) as well as individual devices.

By default, two types of containers are available in the topology view:

- **Tenant**: Top-most container.
- **Undefined**: Container for all devices that have registered themselves with the CloudVision Portal using Zero Touch Provisioning (ZTP) and are awaiting configuration. Undefined containers are shown in the view in a different color than defined containers.

The example shown in Figure 8-1 includes:

- One tenant container (there is always only one tenant container).
- 3 containers under the tenant container (one of the three is an undefined container).
- 7 devices (one is under the undefined container, and 6 are grouped under the container named Vantage-DC (6)).

**Note**

Different color icons are used to indicate that devices have compliance alerts or access alerts. See Viewing Containers and Devices on page 202 for more information about the meanings of the different device icon colors.

For more information, see:

- Network Provisioning Screen Options
- Changing Between Network Provisioning View and List View

**Related topics:**

- Container Level Actions (Create, Rename, Delete)
- Device Level Actions
- Viewing Containers and Devices
8.1.1 Network Provisioning Screen Options

The following options are available from the Network Provisioning screen.

- **Device Management** - Lists all the switches that reside below the selected container level, these could belong to the selected container or reside in containers within the selected container.
- **Configlet Management** - Lists the configlets associated with the selected container or if a switch is selected all of the configlets applied to it both directly and inherited.
- **Image Management** - Lists the EOS or vEOS software image associated with a container or switch. Switches below the container selected will be loaded with this image.
- **Label Management** - Lists the system or custom labels associated with the selected container or switch.
- **Refresh and Listview** - Refresh the current screen to show any updates or changes to the switches or devices. Listview changes the display from Topology View and displays the switches in a list.
- **Containers** - Containers are the basic logical construct of the topology view. They are used to group devices and to apply configurations and deploy images to the device groups.

**Container Right Click Options:**

- **Show From Here** - Changes the display to show only the containers and switches below the selected container.
- **Expand / Collapse** - toggles between shrinking or growing the tree topology below the selected container.
- **Show All Devices** - Lists the switches that are associated with that specific container. The container turns blue if it contains more than five switches and will only display 25 of the total number of switches in the topology structure.
- **Container: Add / Delete** - Create or remove a container that from the selected container.
- **Device: Add / Manage** - Add a device to the selected container or manage the switches already associated with the container. The manage option displays a list of switches which can be selected by enabling the tick box on the left-hand side. The selected switches can then be moved to another container, reset (returned to a ZTP boot state and associated with the undefined container), or removed from CVP completely.
- **Manage: Configlet / Image Bundle** - Allocate or remove a configlet or Image to or from a switch or container.
- **View Config** - View the configuration created from the combined configlets. At the container level this shows the combined configlet configuration associated with that container.
- **Check Compliance** - To initiate a compliance check on all devices under the container.
- **Reconcile** - To initiate configuration reconcile on all devices under the container.

**Device Right Click Options:**

- **Manage: Configlet / Image Bundle** - Allocate or remove a configlet or Image to or from a switch or container.
- **Labels** - Lists / assigns the user created labels associated with the selected switch.
- **View Config** - View the configuration created from the combined configlets. At the switch level the entire configuration that will be applied to the switch is shown.
- **Check Compliance** - Compares the current running configuration on the switch against the designed configuration in CVP. If they are out of sync the device change to an orange color.
- **Move** - Allows a user to move a switch from one container to another.
- Factory Reset - Erases the configuration on the switch then ZTP boots it. This will return it to the undefined container on the provisioning screen.
- Remove - Removes the switch from CVP. This stops CVP making changes to it and tracking its configuration. The switch is left running with its current configuration on it.
- Replace - To perform a Zero Touch Replacement (ZTR) of the selected device.

Related topics:
- Changing Between Network Provisioning View and List View
- Container Level Actions (Create, Rename, Delete)
- Device Level Actions
- Viewing Containers and Devices

8.1.2 Changing Between Network Provisioning View and List View

Figure 8-3 shows the icons you use to toggle between the topology view and the list view of the Network Provisioning page.

8.1.2.1 Changing to List View

Click the list icon for a list view.

Figure 8-2: Changing to List View

8.1.2.2 Changing to Topology View

Click the topology icon for a topology view.
8.2 Container Level Actions (Create, Rename, Delete)

Containers are a logical entity used to group network devices and to define a hierarchy to which configurations can be applied. When you apply a configlet to a container, the configlet is automatically applied to all of the devices in the container's hierarchy.

Simple container implementations:
- Create a container for every datacenter.
- Within each datacenter container, create a container for every POD (leaf-spine deployment).
- Add devices that belong to each POD to the POD container.

For details on how to create, rename, and delete containers, see:
- Creating a Container
- Deleting a Container
- Renaming a Container

Related topics:
- Device Level Actions on page 170
- Viewing Containers and Devices on page 202
- Device Compliance on page 204
- Notifications for Container-level Compliance Checks and Reconciles on page 209
8.2.1 Creating a Container

To create a container:

Step 1  Select a parent container (the container to which you want to add a new container).
Step 2  Right-click the container and choose Add > Container.

The New Container dialog appears.

Step 3  Enter the name of the new container and select OK to create the container.
Step 4  Click Save to apply the changes.

Related topics:
•  Device Level Actions on page 170
•  Viewing Containers and Devices on page 202
•  Device Compliance on page 204

8.2.2 Deleting a Container

Note  Only empty containers can be deleted.

To delete a container:

Step 1  Locate the container to be deleted.
Step 2  Right-click the container and click Remove.

Related topics:
•  Device Level Actions on page 170
•  Viewing Containers and Devices on page 202
•  Device Compliance on page 204

8.2.3 Renaming a Container

To rename a container in a topology:

Step 1  Double-click the name field of the container to open the name field editor.
Step 2  Enter a new, unique name for the container and click Enter to rename the container.
8.3 Device Bootstrap Process

The device bootstrap process is a process that automatically makes un-provisioned devices available for configuration through CVP. Un-provisioned devices automatically boot up in Zero Touch Provisioning mode and register themselves with the CloudVision Portal (CVP). Once they are registered with CVP, devices become available for configuration in the Undefined Container.

The steps of the device bootstrap process are:

**Step 1** Un-provisioned devices boot into Zero Touch Provisioning mode and send out a DHCP request.

**Step 2** The DHCP server then assigns the device an IP Address and returns a URL pointing to the CloudVision portal in the bootfile-name option. The URL to specify is http://IPADDRESS/ztp/bootstrap.

**Step 3** The device executes this bootstrap script and registers itself with the CloudVision Portal. At this point, the device is available in the Undefined Container.

You can now add the device to the destination container of your choice and apply the correct image and configuration to the device.

Related topics:

- Device Level Actions on page 170
- Viewing Containers and Devices on page 202
- Device Compliance on page 204
8.4 **Device Level Actions**

CloudVision Portal (CVP) enables you to provision devices as needed based on your current networking requirements. Some examples of the types of actions you can perform include:

- Adding devices (use this action to add devices from the undefined container to defined containers)
- Moving devices (used this action to move devices from one defined container to another defined container)
- Removing devices (removing devices from the CVP topology)
- Reset devices
- Replace devices

For details on the steps you use to perform these device level actions, see:

- Adding Devices (from Undefined Container)
- Registering Devices
- Moving Devices from one Container to Another Container
- Removing a Device from a Container
- Device Factory Reset

8.4.1 **Adding Devices (from Undefined Container)**

Adding devices from the undefined container is the most common method for adding devices to a container in the CVP topology. This method involves adding devices that are not part of the hierarchy of devices to defined containers in the CVP topology. Containers that receive the added devices are called destination containers.

Complete the following steps to add a device from the undefined container to a destination container:

**Step 1**  Locate the container to which you want to add a device.

**Step 2**  Right-click the container and choose **Add > Device**.

The current inventory of undefined devices for the selected container appears (Figure 8-4 on page 171).
Figure 8-4: Adding a device

Step 3 Select the device and click Add.

Step 4 Save the session.
This automatically spawns a Device Add task.

Step 5 Execute the Device Add task using the Task Management module to add the device to destination container.

8.4.2 Registering Devices

Registering is the method used for adding devices to CVP. As a part of registering devices, CloudVision automatically enables state streaming to the cluster by installing and configuring the TerminAttr agent. Newly registered devices are always placed under an undefined container.

Note Manual installation or configuration of streaming telemetry is not required prior to registration.

Complete the following steps to register devices with CVP:

Step 1 Navigate to the Inventory page.

Step 2 Click the Add Device drop-down menu and select Register Existing Device. See Figure 8-5.
Step 3  Enter the host name or IPv4 addresses of the device(s) to be registered; and click Register. See Figure 8-6.

As a result of registering a device, the streaming telemetry agent will be installed and configured on the registered device and will be listed in the undefined container in the network provisioning view.
The newly registered devices are now shown in the inventory. See Figure 8-9.
The newly registered devices are shown in the undefined container in the Network Provisioning view. See Figure 8-10.

Figure 8-10: Registered Devices in the Network Provisioning View

8.4.3 Moving Devices from one Container to Another Container

Moving devices from one defined container to another is a method you can use to add devices to a container in the CVP topology. You use this method when you want to add devices to a container, and the device you want to add is currently under another container in the CVP topology. This method involves locating the device to be moved, and then moving it to the destination container. Containers that receive the imported devices are called destination containers.

There are three options you can use to move devices. They are:
Chapter 8: Network Provisioning (CVP) Device Level Actions

- Option 1: on page 175
- Option 2: on page 175
- Option 3: on page 176

Option 1:
Step 1 Locate the device.
Step 2 Right-click the device and choose Move.

Figure 8-11: Selecting the device to be moved (option 1)

The Container Info dialog appears.
Step 3 Select the destination container from the drop-down menu.
Step 4 Save the session to move the device to the destination container.

Option 2:
Step 1 Locate the container that has the device you want to move.
Step 2 Right-click the container and choose Show All Devices.

This will load the inventory of all the devices under the container.
Step 3  Locate the device to be moved.

Step 4  Right-click the device and choose Move.

After moving there will be a "T" icon to indicate the move has been tasked. (The task won't automatically be executed.)

Figure 8-12: Device with pending move task (option 2)

Step 5  Go to Tasks and explicitly execute the move task.

After the task has been executed, the “T” icon is removed.

Option 3:

Step 1  Locate the container that has the device you want to move.

Step 2  Right-click the container and choose Manage > Device.

This will load the inventory of all the devices under the container.

Step 3  Select the device to be moved and click “<–>”to choose the destination container.

Step 4  From the popup menu, select the destination container and click OK.

This will provision a move for the device.

8.4.4 Removing a Device from a Container

A device can be removed from a container. Removing a device from the container will:

- Remove the device from parent container.
- Clear all information about the device in the CloudVision Portal.
- Stop any monitoring of the device.

There are three options you can use to remove devices. They are:

- Option 1: on page 176
- Option 2: on page 177
- Option 3: on page 178

Option 1:

Step 1  Locate the device to be removed.

Step 2  Right-click the device and choose Remove.
Figure 8-13: Removing a device (option 1)

Option 2:
This option is available only for topology views.

Step 1  Locate the parent container.

Step 2  Right-click the container and choose Show All Devices.
         All the devices under the container are listed.

Figure 8-14: Selecting the device to be removed (option 2)

Step 3  Select the device you want to remove.

Step 4  Right-click the device and choose Remove.
         The device is removed from the Network Provisioning view.
Option 3:
This option is available only for the list view of the Network Provisioning screen.

**Step 1** Locate the parent container.

**Step 2** Right-click the container and choose **Manage > Device**.

This loads the inventory of all the child devices under the container.

**Figure 8-16: Remove device from the container (option 3)**

**Step 3** Select the device you want to remove and then click **Remove**.
8.4.5 Device Factory Reset

When resetting a device:

- The device will be removed from the parent container.
- The running configuration of the device will be flushed.
- Device will reboot with ZTP mode enabled.
- Device will be identified under undefined container.

There are three options you can use to move devices. They are:

- Option 1: on page 179
- Option 2: on page 179
- Option 3: on page 180

Option 1:

Step 1 Locate the device.
Step 2 Right-click the device and choose Factory Reset.

Figure 8-17: Resetting the device (option 1)

Option 2:

Step 1 Locate the parent container.
Step 2 Right-click the container and choose Show All Devices.
   This will list all the devices under the container.
Step 3   Right-click the device and choose **Factory Reset**.

Option 3:

**Step 1**   Locate the parent container.

**Step 2**   Right-click the container and choose **Manage > Device**.

This will load the inventory of all the child devices under the container.

**Step 3**   Select the checkbox of the device to be reset, and click the reset icon.
On saving the session, a task will be spawned to reset the selected device.
8.5 Replacing Switches Using the ZTR Feature

The Zero Touch Replacement (ZTR) feature enables you to replace switches without having to configure the new switch. When you replace a switch using this feature, the new switch assumes the identity (IP), image, and configuration of the old switch. You use the Network Provisioning page to replace switches using the (ZTR) feature.

Pre-requisites: Before you can begin the process to replace a switch using ZTR, make you must complete the following steps:

Step 1 Make sure that the old switch is physically powered down and is not physically connected to the network.

Step 2 Physically connect the new switch to the network exactly as the old switch was connected.

Step 3 Power on the new switch.

Step 4 Make sure the new switch comes up using ZTP, and that it shows up in the undefined container as an available resource.

Complete these steps to replace a switch using ZTP:

Step 1 Go to the Network Provisioning page.

Step 2 Right-click on the old switch, and select Replace.

Figure 8-21: Selecting the switch to be replaced

This initiates ZTR, and opens the Undefined Device page.

Step 3 Select the new switch by checking the checkbox next to the Serial No. column, and then click Replace.
Figure 8-22: Selecting the new device and replacing the old device

Step 4  In the Network Provisioning page, click **Save**.

A task icon “T” shows on the old switch, indicating that a task to replace it has been scheduled. Also, an “R” icon shows on the new switch, indicating that it is the replacement switch for a scheduled ZTR task.

Figure 8-23: Topology view showing device with pending replace task

Step 5  Go to the Tasks page.

Step 6  Select the task and click the play icon to execute the task.
While the task is executing, you can open the logs for the task to view how ZTR manages the replacement. ZTR first pushes the old switch’s image and configuration to the new replacement switch, and then initiates the reboot.

### 8.6 Managing Configurations

CloudVision Portal (CVP) enables you to manage configurations by assigning configurations to containers and to devices. Configurations that you assign to containers are applied to all devices under the container’s hierarchy. CVP also enables you to easily view the configuration currently assigned to containers and devices.

- **Applying Configurations to Containers**
8.6.1 Applying Configurations to Containers

Applying configurations to containers involves adding Configlets to containers or removing Configlets from containers.

**Adding Configlets:**

*Step 1* Locate the container.

*Step 2* Right-click the container and choose Manage > Configlet.

This will open the window displaying the inventory of configlets.

*Step 3* Select the configlet and click Update.

This will provision configlet add for the container and all the devices under it.

**Removing Configlets:**

To remove the configlet inventory from a container.

*Step 1* Locate the container.

*Step 2* Right-click the container and choose Manage > Configlet.

*Step 3* Remove the configlets.

*Step 4* Click Update.

**Figure 8-26: Remove the configlet and select Update**
8.6.2 Viewing the Configuration Applied to Devices

CloudVision Portal (CVP) enables you to use the Network Provisioning page to view the configuration (Configlets) currently assigned to devices. When you view the Configlets, you can also see which Configlets are inherited from Containers, and which are applied directly to the device.

Complete the following steps to view the Configlets applied to a device.

**Step 1** Go to the Network Provisioning page.

**Step 2** Make sure you are using the topology view, not the list view.

**Step 3** Click on the **device** in the topology.

**Step 4** Click the **Configlet** icon.

The Configlets applied to the device are listed in a drop-down list.

- If a Configlet is inherited from a Container to which the device belongs, the Container icon appears in front of the Configlet name.
- If a Configlet is directly applied to the device, no Container icon is shown next to the Configlet name.

See Figure 8-27 on page 186 for an example.

**Figure 8-27: Viewing the Configlets applied to a device**

---

8.6.3 Applying Configurations to a Device

Applying configurations to devices involves adding Configlets to devices.

**Note** When you update a device configuration using configlets, CVP replaces the entire device configuration with the Designed Configuration for the device. For new devices with pre-existing configurations added into CVP, you must explicitly perform a one-time reconciliation to save the desired device-specific running configuration in CVP. If you do not, that configuration may be lost, or the configuration update task may fail (see Reconciling Device Configurations at the Device Level (page 189)).
Adding Configlets:

**Step 1** Select the device and choose Manage > Configlets.
This loads the configlet inventory page.

**Step 2** Select the configlets.
You are required to validate the configuration.

**Step 3** To validate the configurations, select Validate.
The validation page will be loaded.

**Step 4** Select Save to propose a Config Assign action.
When saving the session, this will spawn a Config Assign task.

8.6.4 Rolling Back Configurations Assigned to a Device
CloudVision’s Network Rollbacks feature enables you to restore a previous configuration to devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the configuration or EOS image (or both).

See Rolling Back Images and Configurations on page 195 for details.

8.7 Configuration Validation
The validation page (Figure 8-28) consists of 3 panes.

- Pane 1: Shows the proposed configuration.
- Pane 2: Shows the designed configuration. (This shows how a resulting running configuration will look like after successful configuration push.)
- Pane 3: Shows the current running configuration of a device.
8.8 Using Hashed Passwords for Configuration Tasks

Some EOS commands take a password or a secret key as a parameter. There are usually two ways of passing EOS command parameters:

- As plain text
- As a hashed string.

Important! Because EOS always returns the hashed version of the command in its running configuration, using the plain text version of commands in Configlets results in the following issues:

- CVP shows that there are configuration differences that need reconciling, even if there are none.
- Compliance checks show devices to be out of compliance.

To avoid these issues, you should use the hashed version of EOS commands in Configlets (for example, use "ntp authentication-key 11 md5 7 <key>" instead of "ntp authentication-key 11 md5 0 <key>" ). Using the hashed versions of commands also keeps the real password hidden.

8.9 Reconciling Configuration Differences

CloudVision enables you to reconcile differences between the designed (managed) configuration and running configuration on devices so that CVP is maintaining the full configuration of each device.
8.9.1 Key Terms

**Reconcilable differences**
Configuration differences between the designed configuration and the running configuration, which do not conflict with the configuration in any configlets, other than the reconcile configlet.

**Reconcile configlet**
A specially marked device configlet that is system generated and used to store reconcilable differences in order for the designed configuration to match the running configuration.

Reconciling device configuration differences does not require a task, because there is no configuration to be pushed out to the device. Reconcilable differences are only adjusted in the reconcile configlet, to match the running configuration. Because of this, there is no task pushed to change the running configuration.

When you reconcile device configuration differences, you add the reconcilable differences found in the running configuration to the reconcile configlet of the designed configuration.

For details on reconciling device configuration differences, see:
- Reconciling Device Configurations at the Device Level on page 189
- Reconciling Device Configuration Differences at the Container Level on page 191

8.9.2 Reconciling Device Configurations at the Device Level

CloudVision enables you to reconcile device configuration differences at the device level (specific, individual devices). Configuration differences at the device level occur when there are reconcilable differences in the running configuration of the device.

The Configuration Validation page shows details of the configuration differences. When the system identifies a reconcilable difference, the “Reconcile” option becomes available, and the extra reconcilable configuration is listed in a text editor on the page (see Figure 8-29 on page 190).

**Reconcile Configlets**

You use a type of configlet called a reconcile configlet to reconcile device configuration differences at the device level. A reconcile configlet is a configlet for a single, specific device, and is explicitly marked as the reconcile configlet for that device. The reconcile configlet for a device contains the extra running configuration for that device.

**Note**
There is only one reconcile configlet for any device. It is the only configlet that contains the extra running configuration for the device.

Every time a device-level or a container-level reconcile is performed, the reconcile configlet for each device included in the reconcile action is modified to include the extra running configuration.

See Figure 8-29 on page 190 for an example of the Configuration Validation page showing device-level configuration differences.
Step 1  Click the blue **Reconcile** button to add the reconcilable configuration in the running configuration to the reconcile configlet of the designed configuration.

Step 2  (Optional) Click the **Reconcile disk icon** at the top beside the configlet to save the reconcile configlet with the extra commands present in the running configuration.

**Note**  CVP will not execute pushing a configuration that causes CVP to lose connectivity with the device if the management interface or IP is missing in the configuration. When the task is executed, it will fail.
Reconciling Device Configuration Differences at the Container Level

CloudVision enables you to reconcile device configuration differences for all devices under the hierarchy of a selected container, instead of having to initiate this device by device.

**Note**

The designed configurations of devices in the container that do not have reconcilable differences are not changed.

For devices that have reconcilable differences, the lines or commands on the device that are not present in the designed configuration are pulled into the reconcile configlet for that device in one of two ways:

- Using the existing reconcile configlet that is specific to that device.
- Creating a new reconcile configlet that is specific to that device. This is done when there is no existing reconcile configlet specific for the device. The system automatically creates a unique name for the configlet.

A green checkmark beside the configlet indicates it as the reconcile configlet for the device.

Complete the following steps to reconcile device configuration differences for a container:

**Step 1** Go to the Network Provisioning page.

**Step 2** Locate the container in the topology where you want to reconcile the configurations of all devices under that container hierarchy.

**Step 3** Right-click the container and choose **Reconcile** (see Figure 8-30 on page 191).

Figure 8-30: Device configuration reconciliation at the container level

The configuration of the devices in the container are reconciled. The bell icon in the upper right corner turns yellow to indicate unread notifications.
Step 4  (Optional) To view the notification for the reconciliation, click the bell icon.

The notification list appears showing the container-level configuration reconciliation, and any other unread notifications (see Figure 8-31).

Figure 8-31: List of unread notifications
8.10 Managing EOS Images Applied to Devices

CloudVision enables you to efficiently manage the EOS images of devices by assigning image bundles to containers or devices in the current CloudVision network topology. An image bundle assigned to containers are automatically applied to all devices under that container.

The image bundle you want to apply must already exist in the set of current EOS image bundles. Refer to Chapter 11 for information on how to upload EOS images into CVP.

The following tasks are involved in managing the EOS image bundles assigned to devices:

- Applying an Image Bundle to a Container
- Viewing the Image Bundle Assigned to Devices
- Applying an Image Bundle to a Device
- Setting up an Image Bundle as the default for ZTP
- Rolling Back the Image Assigned to a Device

8.10.1 Applying an Image Bundle to a Container

An image bundle can be added to, or removed from a container.

**Step 1** Select the container and choose **Manage > Image Bundle**.

This will load image bundle inventory in topology (Figure 8-32).

Figure 8-32: Image bundle inventory

<table>
<thead>
<tr>
<th>Image Bundle - AnyCloud</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Containers</td>
<td>Notes</td>
<td>Uploaded by</td>
<td>Uploaded Date</td>
</tr>
<tr>
<td>EOS-4.20.11.1M.swi</td>
<td>0</td>
<td></td>
<td>cvpadmin</td>
<td>2019-02-11 15:27:20</td>
</tr>
<tr>
<td>EOS-4.20.15F</td>
<td>0</td>
<td></td>
<td>cvpadmin</td>
<td>2019-03-27 23:14:22</td>
</tr>
<tr>
<td>TestBundle</td>
<td>0</td>
<td>Testing A0</td>
<td>a</td>
<td>2016-11-28 20:00:52</td>
</tr>
<tr>
<td>EOS-4.21.3F-2GB</td>
<td>0</td>
<td></td>
<td>cvpadmin</td>
<td>2019-03-27 23:15:19</td>
</tr>
<tr>
<td>EOS-4.21.2F-2GB</td>
<td>0</td>
<td></td>
<td>cvpadmin</td>
<td>2019-03-27 23:14:48</td>
</tr>
<tr>
<td>EOS-4.20.11M</td>
<td>2</td>
<td></td>
<td>cvpadmin</td>
<td>2019-03-31 08:33:15</td>
</tr>
<tr>
<td>EOS-4.20.8M.swi</td>
<td>1</td>
<td></td>
<td>cvpadmin</td>
<td>2018-10-04 02:06:45</td>
</tr>
</tbody>
</table>

**Step 2** Select the bundle to be assigned to the container.

**Step 3** Click **Update** to provision the bundle add for the container.

This action will cause a task to be created for each device in the container to upgrade it to the specified image bundle.
8.10.2 Viewing the Image Bundle Assigned to Devices

CloudVision Portal (CVP) enables you to use the Network Provisioning page to view the image bundle currently assigned to a device. You can also see if the image bundle is inherited from a Container or assigned directly to the device.

Complete the following steps to view the image bundle applied to a device.

**Step 1** Go to the Network Provisioning page.

**Step 2** Make sure you are using the topology view, not the list view.

**Step 3** Click on the device in the topology.

**Step 4** Click the image icon in the left pane.

The image bundle assigned to the device is shown in a pop-up box.

- If the image bundle is inherited from a Container to which the device belongs, the Container icon appears in front of the image bundle name.
- If the image bundle is assigned directly to the device, there is no Container icon in front of the image bundle name.

See Figure 8-33 for an example.

Figure 8-33: Viewing the Image Bundle assigned to a device

8.10.3 Applying an Image Bundle to a Device

**Step 1** Right-click the device, then choose Manage > Image Bundle.

This will open the window display the inventory of Image bundles.

**Note**

Only one image bundle can be selected and assigned to a device at a time.

**Step 2** Select the bundle to be assigned to the device.

**Step 3** Click Update to provision the bundle add for the device.
This action will cause a task to be created for that device to upgrade it to the specified image bundle.

8.10.4 Setting up an Image Bundle as the default for ZTP

Since all devices must run this image, you must apply the image at the tenant level.

**Step 1** Go to the Network Provisioning page.

**Step 2** Right-click the **Tenant** container and choose **Manage > Image Bundle**.

**Step 3** Select the bundle you created and click **Update**.

**Step 4** Click **Preview** to verify the changes before saving the changes.

**Step 5** Click **Save** to apply the changes.

8.10.5 Rolling Back the Image Assigned to a Device

CloudVision’s Network Rollbacks feature enables you to restore a previous EOS image to devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the EOS image or configuration (or both).

See [Rolling Back Images and Configurations](#) for details.

8.11 Rolling Back Images and Configurations

CloudVision’s Network Rollbacks feature enables you to restore a previous EOS image and configuration to containers and devices. You can apply the rollback to all the devices in a container, or to single devices. When you rollback a container or device, you select the date and time for the rollback and whether you want to rollback the EOS image or configuration (or both).

CloudVision supports rollback to any previous point in time irrespective of captured snapshots. However, rollback is possible to a point that is far beyond the CloudVision Cluster update to 2018.2.0 only when your devices are upgraded to TerminAttr 1.4+ long before that.

**Note** To help you select the desired rollback destination day and time, you can compare the image and running configuration differences between current and rollback times of all effected devices. The potential destination rollback date and time in the comparison is based on the destination rollback date and time you select.

8.11.1 Rolling Back Device Images and Configurations

Complete the following steps to apply a rollback in devices:

**Step 1** Go to the Network Provisioning page.

**Step 2** Right-click on the device you want to rollback, and then choose **Manage > Rollback**.

The device Rollback page appears. See **Figure 8-34**.
**Step 3**  Using the **Rollback Type**: options near the top of the page, select the type of rollback. The options are:

- Configuration & Image Rollback (both the configuration and EOS image are rolled back)
- Configuration Rollback (only the configuration is rolled back)
- Image Rollback (only the EOS image is rolled back)

**Step 4**  Either drag the vertical slider on the timeline to the desired date and select the time for rollback; or use the **Rollback to** menu for selecting rollback date and time (directly above the **configuration** pane on the left side).

**Step 5**  Click the telemetry icon (directly above the **configuration** pane on the right side) for viewing the running configuration differences between current and rollback times. See Figure 8-35.

---

**Figure 8-35: Differences in Running Configuration**
The **Unified** tab displays running configuration differences in a single window with differences highlighted. The **Split** tab displays running configurations in different windows with differences highlighted.

**Step 6** If required, change the destination date and time for the rollback.

**Step 7** Click **Save** to create a task for the device rollback.

### 8.11.2 Rolling Back Container Images and Configurations

**Step 1** Go to the Network Provisioning page.

**Step 2** Right-click on the container you want to rollback, and then choose **Manage > Network Rollback**.

The Network Rollback page appears. See **Figure 8-36**.

**Figure 8-36: Network Rollback Page**

**Step 3** Using the **Rollback Type**: options near the top of the page, select the type of rollback. The options are:

- Configuration & Image Rollback (both the configuration and EOS image are rolled back)
- Configuration Rollback (only the configuration is rolled back)
- Image Rollback (only the EOS image is rolled back)

**Step 4** Either drag the vertical slider on the timeline to the desired date and select the time for rollback; or use the **Rollback to** menu for selecting rollback date and time (directly above the configuration pane on the left side).

**Step 5** Click the telemetry icon (directly above the configuration pane on the right side) for viewing the running configuration differences between current and rollback times. See **Figure 8-35**.

**Step 6** If required, change the destination date and time for the rollback.
Step 7  Click **Create CC** to create a Change Control (CC) record for the network rollback. CloudVision automatically creates a rollback task for each device in the rollback; and makes them part of CC.

**Note**  Rollback Change Controls are automatically assigned a unique name. You can rename the Change Control record by editing the Change Control record. Once the Change Control is created, it can be scheduled or executed like any other Change Control. See **Using the Change Control Module to Manage Tasks on page 276** for details.

## 8.12 Device Labels

A label is simply defined as Text Tags. There are two types of label:

- **System labels**: Assigned automatically by the system.
- **Custom labels**: Defined and assigned by the user.
  - Users can assign custom labels to devices from the Network Provisioning page.
  - A device can be tagged with one or more custom labels.
  - Labels can be used to filter the devices in the Network Provisioning page.

### 8.12.1 System Labels

System labels are defined by the system and are automatically applied to and removed from devices based on the following characteristics of that device:

- Software version
- Software bundle
- Product model and family
- Assigned configlet name
- DANZ enabled
- MLAG enabled
- Parent container name

**Note**  System labels cannot be modified or removed by the user.

### 8.12.2 Custom Device Labels

You can create custom device labels and assign them to devices. The device labels you assign to a device show on the Network Provisioning page next to the device.

#### 8.12.2.1 Assigning an existing label to a device

Complete these steps to assign an existing label to a device.

**Step 1**  Select the device to be labeled.
Step 2  Right-click the device and choose **Labels**.

The Assign Label pop-up menu appears, showing the available device labels.

Step 3  Select the label to be applied and click **Save**.

The selected label will be applied to the device.

8.12.2.2  Creating a Custom Label for a Device

Complete these steps to create a new, custom label to a device.

Step 1  Select the device for which you want to create a new, custom label.
Step 2  Right-click the device and choose **Labels**.

The Assign Label pop-up menu appears, showing the available device labels.

Step 3  In the pop-up menu, click on **CREATE LABEL**.

The Create Label dialog appears.
Step 4  Type the new, custom label for the device, then click **Save**.

![CREATE LABEL](image)

The new label is created and is assigned to the device.

8.12.3  Left Pane Behavior in Network Provisioning View

The left pane in the topology view is used to display information on the resources assigned to a given device or container (see Figure 8-37).

**Figure 8-37: Left pane view**

Opening and Closing the Left Pane

**Step 1**  Double click the container or device to open the left pane.

**Step 2**  Click the “X” button to close it.

8.12.4  Right Pane Behavior in List View

Similar to the left pane in the Network Provisioning View, the right pane in the List view is used to display information regarding resources assigned to the given device or container (see Figure 8-38 on page 202).
8.13 Viewing Containers and Devices

The Network Provisioning page provides you with various options that enable you to easily control the topology view so that you can view containers and devices based on your needs.

The options you use are:

- Expand / Collapse (see Expanding and Collapsing Containers)
- Show From Here (see Show From Here on page 203)
- Show Full Topology (see Show Full Topology on page 203)

CloudVision Portal uses color coded icons to indicate compliance or access issues with devices. See Device Compliance Status Indicators on page 204 and Device Access Alerts on page 208 for more information.

8.13.1 Expanding and Collapsing Containers

Containers can be expanded and collapsed within the Network Provisioning topology view so that you can change the view as needed based on your needs.

You use the “Show From Here” and “Show Full Topology” options to expand or collapse containers shown in the Network Provisioning screen.

The “Expand and Collapse” option is only available for the Network Provisioning view. It is not available for the List view.
The default view mode for containers is expanded. When you choose Expand / Collapse option for a container, one of the following occurs, depending on the current view mode:

- A container currently in expanded (normal) view is collapsed.
- A container currently in collapsed mode is returned to expanded view mode (the default).

**Figure 8-39: Expanded and collapsed view of a container**

Complete these steps to expand or collapse a container view from the Network Provisioning page.

**Step 1**  Select a container.

**Step 2**  Right-click it and select the “Expand/Collapse" option.

### 8.13.2 Show From Here

The “Show From Here” option displays the topology with the selected container as the root. The hierarchy above the selected container will be hidden from the view allowing the user to only focus on the chosen container and the tree below it.

**Step 1**  Select a container.

**Step 2**  Right click “Show From Here” to display the option.

The hierarchy from the selected container will be displayed.

### 8.13.3 Show Full Topology

The “Show Full Topology” option allows the user to get back to the full topology view. This option will be enabled for a particular container once the user uses the show from here option on it.

**Step 1**  Select a container.

**Step 2**  Right-click “Show Full Topology” to view the option.
## 8.14 Device Compliance

In CloudVision Portal (CVP), devices have a compliance status which indicates whether the running configuration and image of a device is different from the designed (managed) configuration and image for the device.

The possible device compliance statuses are:

- **Compliant**: Devices in which the running configuration and image are identical to the designed configuration and image for the device.

- **Non-compliant**: Devices in which the running configuration or image are different from the designed configuration or image for the device.

CVP enables you to check devices to determine if they are non-compliant. It also provides device compliance status indicators so you can easily identify non-compliant devices and the functionality required to bring non-compliant devices into compliance. One process used to resolve the difference in running and designed configuration is referred to as reconciling.

For more information, see:

- [Device Compliance Status Indicators](#)
- [Device Compliance Checks on page 207](#)
- [Reconciling Configuration Differences on page 188](#)

### 8.14.1 Device Compliance Status Indicators

CloudVision Portal (CVP) provides device compliance status information in both the Network Provisioning page and the Inventory page (list view).

- [Network Provisioning Page Compliance Status Indicators](#)
- [Representation Under “Show All Devices” on page 206](#)

#### 8.14.1.1 Network Provisioning Page Compliance Status Indicators

The Network Provisioning page (topology view) utilizes color coding to indicate the presence of compliance alerts on devices. A compliance alert on a device indicates that the running configuration or image is different from the designed configuration or image for the device. This feature enables you to easily see if a device has a compliance alert.

In addition to using color codes for device icons, CVP also uses color codes for container icons to indicate that a device within the container has a compliance alert. If a device within a container has an active alert, the container inherits the alert color of the device. For example, if a device within a container has a configuration mismatch, the container inherits the alert color used to indicate a configuration mismatch.

This feature enables you to easily see if a device within a container has an alert, even if the device is not visible. It also prevents you from having to open a container to see if a device within it has an alert.

For descriptions of the color codes used to indicate compliance status, see:

- [Device icon compliance status color codes on page 205](#)
- [Container icon compliance status color codes on page 205](#)
Device icon compliance status color codes

The color of the device icon indicates the compliance status of the device. This table lists and describes the device icon color codes:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gray</td>
<td>The compliance status is normal (no compliance alert).</td>
</tr>
<tr>
<td>Orange (no task)</td>
<td>The device has a configuration mismatch (the running configuration or image are different from the designed configuration or image for the device). No task to resolve the mismatch is associated with the device.</td>
</tr>
<tr>
<td>Orange (with task)</td>
<td>The device has a configuration mismatch (the running configuration or image are different from the designed configuration or image for the device). A task to resolve the mismatch is associated with the device.</td>
</tr>
</tbody>
</table>

See Representation Under “Show All Devices” on page 206 for how this status is shown when using the Show All Devices option.

Container icon compliance status color codes

Figure 8-40 shows a container that has a device within it that has an alert. In this example, the alert color is yellow, which indicates one of the following:

- A device within the container has a configuration mismatch.
- A device within the container has a configuration mismatch, and there is a task associated with the device to resolve the mismatch.

Figure 8-40: Container showing alert color
8.14.1.2 Representation Under “Show All Devices”

Figure 8-41 shows the representation of device compliance status information for devices that are only visible by accessing “Show all devices”. The statuses shown are the same as those shown using device icons in the topology view (see Device Compliance Status Indicators on page 204).

Figure 8-41: Show All Devices display of device compliance status

8.14.1.3 Representation in List View

Figure 8-42 shows the representation of device compliance status information when using the List View. The statuses shown are the same as those shown using device icons in the topology view (see Device Compliance Status Indicators on page 204).

Figure 8-42: List View display of device compliance status

8.14.1.4 Removing Compliance Indicators

The Network Provisioning page shows non-compliance whenever there is a mismatch between the running configuration or image and designed configuration or image of devices in the topology. Compliance indicators are removed from the display only when there is no configuration mismatch.
To remove compliance indicators, you may need to do one or more of the following:

- Run a compliance check on any devices on which there is no configuration mismatch.
- Run a task to bring any non-compliant devices into compliance.
- Reconcile the configuration of any devices that have a configuration mismatch.

### 8.14.2 Device Compliance Checks

CloudVision Portal (CVP) enables you to see if devices are non-compliant by performing compliance checks at the device level and at the container level.

#### 8.14.2.1 Running container-level compliance checks

When you run a compliance check at the level of the container, CloudVision Portal (CVP) compares the running configuration and image on each device in the container against the designed configuration and image for each device in the container. You run the check from the Network Provisioning page.

When you start the compliance check, a message at the top of the page indicates that the check has started. When the check is done, non-compliant devices are indicated on the page using colors (yellow or red). In addition, CVP automatically generates a notification that a compliance check has been completed. You can view the notification for the compliance check by clicking the bell icon on the page.

Complete these steps to run a container-level compliance check:

**Step 1** Make sure the Network Provisioning tab is selected.

**Step 2** On the Network Provisioning page, locate the container to be checked for compliance.

**Step 3** Right-click on the container and choose **Check Compliance** (see Figure 8-43).

**Figure 8-43: Container-level compliance check**

---

Configuration Guide: CloudVision version 2018.2.3 207
8.14.2.2 Running device-level compliance checks

When you run a compliance check on a single device, CloudVision Portal (CVP) compares the running configuration and image on the device against the designed configuration and image for the device. You run the check from the Network Provisioning page.

Complete these steps to run a device-level compliance check:

**Step 1** Make sure the Network Provisioning tab is selected.

**Step 2** On the Network Provisioning page, locate the device on which you want to run the compliance check.

**Step 3** Right-click on the device and choose **Check Compliance**.

CVP initiates the compliance check. Non-compliant devices are indicated on the page using device compliance status icons (see **Device Compliance Status Indicators** on page 204).

8.14.3 Device Access Alerts

The Network Provisioning page shows device access alerts whenever a device is no longer reachable by CVP. This enables you to easily identify unreachable devices in the page. Any device that is no longer reachable is represented on the page using a color coded device icon.

This table lists and describes the color codes used for unreachable devices:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
</table>
| ![Icon] | Red  
The device is unreachable (CVP cannot connect to the device). |

Like device compliance status alerts, CVP also uses color codes for container icons to indicate that a device within the container is unreachable. If a device within a container has an access alert, the container inherits the alert color of the device (red).

This feature enables you to easily see if a device within a container has an alert, even if the device is not visible. It also prevents you from having to open a container to see if a device within it has an alert.

**Note**  
Containers only inherit the alert color of a device if the device is directly underneath the container in the hierarchy. If the device is not directly underneath the container in the hierarchy, the container does not show the alert notification color of the device.
8.15 Notifications for Container-level Compliance Checks and Reconciles

CloudVision Portal (CVP) provides notifications for container-level compliance checks and reconciles. When a container-level compliance check or reconcile is completed, CVP automatically generates a notification message, indicating that the action has occurred.

Because container-level compliance check or reconciles are not tracked by tasks, you track them using automated notifications. The notifications can be accessed directly from the Network Provisioning page by clicking the Notifications icon. The presentation of the icon indicates whether there are unread notifications.

The notification list provides the following information:

- Current actions in progress, with a progress bar.
- Unread notifications (shaded in blue).
- Previously viewed notifications (no shading). These are shown at the bottom of the list.

The type of action (Check Compliance or Reconcile) is indicated for each notification.

**Figure 8-44: List of notifications**

**Note**

To view notifications for the previous CVP session, click the bell icon and choose View History.

For information on container-level compliance checks and reconciles, see:

- Device Compliance Checks on page 207
- Reconciling Device Configuration Differences at the Container Level on page 191.
8.16  Global Search
In the Network Provisioning module, the user can use the search bar at the top of the module to find a given device or container.

8.16.1  Search behavior in Topology and List View
This search is very different from rest of other search options available in topology. On user starts to type, the list of possible matches will be displayed below as an auto suggestion.

8.16.2  Topology Search

8.16.3  List View Search
The search behaves similar to the topology search.
For a single device search, the selected device will be listed in the grid.
8.16.4 "Search" in Other Grids

During a grid search, the user will not be provided with an auto suggest option. Only the records matching the specified data entered will be filtered and displayed in the grid.

Figure 8-47: Grid searches

8.16.5 Label Search

Use the search bar from the Network Provisioning page to filter the devices based on labels. This is a contextual search.
To search a label:

**Step 1** Use the keyword “Label:” followed by the label name.

**8.16.5.1 AND Operation**

Lists all the devices which has both the labels present on it in the hierarchy.

Label: <Label Name> AND Label: <Label Name>

*Figure 8-48: Search AND operation*

**8.16.5.2 OR Operation**

Lists all the devices which has either one of the labels present on it in the hierarchy.

Label: <Label Name> OR Label: <Label Name>

*Figure 8-49: Search OR operation*

**8.16.5.3 NOT Operation**

Lists all the devices which has first label one the labels present on it in the hierarchy.

Label: <Label Name> AND NOT Label: <Label Name>
Figure 8-50: Search AND NOT operation
8.16.6  Preview Option

All the actions performed in Network Provisioning module can be previewed before saving the changes.

To access the preview page:

**Step 1**  Select the “Preview” button.

Figure 8-51: Preview option display

8.17  Management IP

The CloudVision Portal tracks the Management IP of each device to use in connecting to it. When this IP address changes, the device becomes unreachable by the portal. You can manually change the IP address used by the portal to communicate with a given device.

8.17.1  Changing A Device's Management IP

The management IP address of a device may change for one of the following reasons:

**Reason 1:**

When a device is provisioned using Zero Touch Provisioning, it may have been assigned a temporary IP address via DHCP. The CloudVision Portal will use this IP address to provision the device. Once the configuration is pushed and the device reboots, this IP address may change.

**Reason 2:**

If you change the device IP address directly via the switch console, CloudVision cannot record the change, and the device will become unreachable. **Current management IP** and **proposed management IP** can be used to mitigate this potential issue.

**Option 1:**

Current Management IP: The IP address used by CloudVision to communicate with a device.

**Step 1**  Set the proposed IP address before pushing the configlet. This way CloudVision will try to reach the device with this IP address once configuration is pushed.
Option 2:
Proposed Management IP: The IP address that CloudVision uses after pushing the configlet.

**Step 1** In the Inventory Management page and the topology, update the Management IP address. For any unreachable device, set the IP address to bring it back to the network.

8.17.2 Setting Proposed Management IP

You can set the Proposed Management IP while adding configlets to the device using the Proposed Management IP menu (see Figure 8-52 and Figure 8-53).

Figure 8-52: Location of menu for setting Proposed Management IP

If you do not set the Proposed Management IP, you cannot save the configuration as not setting Proposed Management IP.
Step 1  Select the Proposed Management IP using the drop-down menu. CloudVision lists the available Management IP, Loop back IP, VLAN IP, and Routed Ethernet IP.

Step 2  Select the desired IP address.

Step 3  Click Save. A task is spawned to assign the new Proposed Management IP.

8.17.3 Changing Current Management IP

Step 1  Go to the Network Provisioning page.

Step 2  Select a device from topology/list view.
Step 3  Right-click the device and choose Manage > IP Address.

Step 4  A pop up will appear allowing you to manually add a new IP address.

Step 5  Verify the reachability of new IP address.