# Compliance Audit for Network Devices



## Compliance Overview

Compliance helps in identifying any intent deviation or *out-of-band* changes in the network that may be injected or reconfigured without affecting the original content.

A network administrator can conveniently identify devices in Cisco DNA Center that do not meet compliance requirements for the different aspects of compliance, such as software images, PSIRT, network profiles, and so on.

Compliance checks can be automated or performed on demand.

- Automated compliance check: Uses the latest data collected from devices in Cisco DNA Center. This compliance check listens to the traps and notifications from various services, such as inventory and SWIM, to assess data.
- Manual compliance check: Lets you manually trigger the compliance in Cisco DNA Center.
- Scheduled compliance check: A scheduled compliance job runs every day at 11:00 pm and triggers the compliance check for devices on which the compliance check was not run in the past seven days.

# Types of Compliance

| Compliance Type | Compliance Check | Compliance Status |
|---|---|---|
| Startup versus Running Configuration | This compliance check helps in identifying whether the startup and running configurations of a device are in sync. If the startup and running configurations of a device are out of sync, compliance is triggered and a detailed report of the out-of-band changes is displayed. The compliance for startup vs. running configurations is triggered within 2 minutes of any out-of-band changes.<br>**Note** Cisco DNA Center must be configured as a Syslog server in **Design** > **Network Settings** > **Telemetry** > **Syslogs** window for Syslog based collection to work. | • Noncompliant: The startup and running configurations are not the same. In the detailed view, the system shows different startup vs. running between or running vs. previous running.<br>• Compliant: The startup and running configurations are the same.<br>• NA (Not Applicable): The device, such as AireOS, is not supported for this compliance type. |
| Software Image | This compliance check helps a network administrator to see if the tagged golden image in Cisco DNA Center is running on the device. It shows the difference between the golden image and the running image for a device. When there is a change in the software image, the compliance check is triggered immediately without any delay. | • Noncompliant: The device is not running the tagged golden image of the device family.<br>• Compliant: The device is running the tagged golden image of the device family.<br>• NA (Not Applicable): The golden image is not available for the selected device family. |
| | For Cisco Switch Stacks: Cisco DNA Center allows the network administrator to check if the tagged golden image is running on the primary switch and members of switch stacks. | • Noncompliant: The tagged golden image is not running on the primary switch and member switches.<br>Also, the device will be noncompliant, if no golden tagging is applicable for the device, and the member switches are not running on the image version as that of the primary switch.<br>• Compliant: The tagged golden image is running on the primary switch and member switches.<br>Also, the device will be compliant, if no golden tagging is applicable for the device, and the member switches are running on same image version as that of the primary switch.<br>• NA (Not Applicable): The golden image is not applicable for the device and the device is not a stacked switch. |

| Compliance Type | Compliance Check | Compliance Status |
|---|---|---|
| Critical Security (PSIRT) | This compliance check enables a network administrator to check whether the network devices are running without critical security vulnerabilities. | • Noncompliant: The device has critical advisories. A detailed report displays various other information.<br>• Compliant: There are no critical vulnerabilities in the device.<br>• NA (Not Applicable): The security advisory scan has not been done by the network administrator in Cisco DNA Center, or the device is not supported. |
| Network Profile | Cisco DNA Center allows you to define its intent configuration using network profiles and push the intent to the device. If any violations are found at any time due to *out-of-band* or any other changes, this check identifies, assesses, and flags it off. The violations are shown to the user under **Network Profiles** in the compliance summary window.<br>**Note** Network profile compliance is applicable for routers, switches and wireless controllers. | • Noncompliant: The device is not running the intent configuration of the profile.<br>• Compliant: While applying a network profile to the device, the device configurations that are pushed through Cisco DNA Center are actively running on the device.<br>• Error: The compliance could not compute the status because of an underlying error. For details, see the error log. |
| Fabric (SDA)<br>This feature is in beta. | Fabric compliance helps to identify fabric intent violations, such as any out-of-band changes for fabric-related configurations.<br>Fabric compliance status does not participate in determining overall compliance status of the device, as the feature is in beta stage. | • Noncompliant: The device is not running the intent configuration.<br>• Compliant: The device is running the intent configuration. |
| Application Visibility | Cisco DNA Center allows you to create an application visibility intent and provision it to a device through CBAR and NBAR. If there is an intent violation on the device, this check identifies, assesses, and shows the violation as compliant or noncompliant under the **Application Visibility** window.<br>The automatic compliance checks are scheduled to run after 5 hours of receiving traps. | • Noncompliant: The CBAR/NBAR configuration is not running on the device.<br>• Compliant: The intent configuration of CBAR/NBAR is running on the device. |
| Model Config | This compliance check enables the network administrator to check any mismatch from the designed intent of Model Config. The mismatch is shown under **Network Profile** in the **Compliance Summary** window. | • Noncompliant: There is a mismatch in the actual and intended value of attributes in Model Config.<br>• Compliant: The attributes in Model Config match the intended value. |

| Compliance Type | Compliance Check | Compliance Status |
|---|---|---|
| CLI Template | Cisco DNA Center allows the network administrator to compare the CLI template with the running configuration of the device. The mismatch in the configuration is flagged. The mismatch is shown under **Network Profile** in the **Compliance Summary** window.<br><br>The running configuration for CLI template compliance is taken from the latest archive that is available for the device. Event-based archive takes at least 2 minutes to update after traps are received. For accurate results, we recommend that you wait for at least 2 minutes before running compliance manually after a configuration change.<br><br>Cisco DNA Center must be configured as a Syslog server in **Design** > **Network Settings** > **Telemetry** > **Syslogs** window for Syslog based collection to work.<br><br>**Note** There are some limitations in CLI template compliance. See Limitations in CLI Template Compliance, on page 10. | • Noncompliant: There is mismatch between the CLI template and the running configuration of the device.<br><br>• Compliant: There is no mismatch between the CLI template and the running configuration of the device. |
| EoX - End of Life | Cisco DNA Center allows you to check compliance status for hardware, software, and module of EoX devices. You can check the EoX compliance status from the **Compliance Summary** > **EoX - End of Life** tile.<br><br>You can also view the EoX status of devices from the **Inventory** window, under the **EoX Status** column.<br><br>**Note** To enable access to the EoX feature, authorize the CX Cloud Consent to Connect agreement through the Cisco DNA Center dashboard. | • Compliant: The device is compliant if enough time remains until the last date of support.<br><br>• Noncompliant: The device is noncompliant if the last date of support has ended.<br><br>• Compliant with Warning: The device is compliant with warning if the last date of support is nearing. |

| Compliance Type | Compliance Check | Compliance Status |
|---|---|---|
| Network Settings | Cisco DNA Center allows you to define its intent configuration settings using network settings and push the intent to the device. If any violations are found at any time due to out-of-band or any other changes, compliance check identifies, assesses, and flags it off.<br>You can view the violations under **Network settings** in the **Compliance Summary** window.<br>**Note** Post UI upgrade, compliance for network settings will get triggered after six hours. | • Compliant: The intent configuration that are pushed are actively running on the device.<br>• Noncompliant: The device is not running the intent configuration.<br>• NA (Not Applicable): The device is not configured with network settings, or the device is not assigned to the site. |
| Cisco Umbrella | Cisco DNA Center allows you to identify the deviation from the intent Cisco Umbrella configuration pushed to the device by Cisco DNA Center. If any violations are found compliance check identifies, assesses and flags it off.<br>You can view the violations under **Workflow** in the **Compliance Summary** window.<br>**Note** Cisco Umbrella compliance check is applicable for Switches or Cisco Embedded Wireless Controllers. Ensure the device provisioning is completed.<br>Also, Cisco Umbrella must be provisioned on the devices. For more information, see Provision Cisco Umbrella on Network Devices. | • Compliant: The intent configuration that are pushed are actively running on the device.<br>• Noncompliant: Device is not running the intent configuration.<br>• NA (Not Applicable): Cisco Umbrella is not configured for the device. |

# View Compliance Summary

The inventory page shows an aggregated status of compliance for each device.

**Step 1** From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The compliance column shows the aggregated compliance status of each device.

**Step 2** Click the compliance status to launch the compliance summary window, which shows the following compliance checks applicable for the selected device:

- Startup versus Running Configuration
- Software Image
- Critical Security Vulnerability

- Network Profile
- Network Settings
- Fabric
- Application Visibility
- EoX - End of Life
- Cisco Umbrella

**Note** Network Settings, Network Profile, Fabric, and Application Visibility are optional and are displayed only if the device is provisioned with the required data.

# Manual Compliance Run

You can trigger a compliance check manually in Cisco DNA Center.

**Step 1** From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

**Step 2** For a bulk compliance check, do the following:

a) Choose all the applicable devices.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

**Step 3** For a per-device compliance check, do the following:

a) Choose the devices for which you want to run the compliance check.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

c) Alternatively, click the compliance column (if available) and then click **Run Compliance**.

**Step 4** To view the latest compliance status of a device, do the following:

a) Choose the device and inventory. See Resynchronize Device Information.

b) From the **Actions** drop-down list, choose **Compliance** > **Run Compliance**.

**Note**

- A compliance run cannot be triggered for unreachable or unsupported devices.
- If compliance is not run manually for a device, the compliance check is automatically scheduled to run after a certain period of time, which depends on the type of compliance.
- CLI Template Compliance compares the realized templates against the running configuration of the device. The running configuration is taken from the latest archive that is available for the device.
- Event-based archive takes at least 2 minutes to update after traps are received. For accurate results, we recommend that you wait for at least 2 minutes before running compliance manually after a configuration change.
- Cisco DNA Center must be configured as a Syslog server in **Design** > **Network Settings** > **Telemetry** > **Syslogs** window for Syslog based collection to work.

# Generate a Compliance Audit Report for Network Devices

Cisco DNA Center allows you to retrieve a consolidated Compliance Audit Report that shows the compliance status of individual network devices. With this report, you can get complete visibility of your network.

For more information, see "Run a Compliance Report" in the *Cisco DNA Center Platform User Guide*.

# Acknowledge Compliance Violations

Cisco DNA Center lets you acknowledge less-important compliance violations of the device and opt-out the violations from the compliance status calculation. If required, you can also choose to opt-in the violation for the compliance status calculation.

**Step 1** From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

**Step 2** Click the device name to open a dialog box that provides high-level information for that device. Click **View Device Details** link in the dialog box.
The device details window is displayed.

**Step 3** In the left pane, choose **Compliance** > **Summary**.

**Step 4** In the **Compliance Summary** window, click the compliance tile for which you want to acknowledge the violations.

You can view the following information under **Open Violations** and **Acknowledged Violations** table:

- Model Name
- Attribute
- Status: This column shows one of the following status:
  - **Added**: The attribute is added in the device.
  - **Changed**: The intent value does not match the device value.
  - **Removed**: The intent is removed from the device.
- Intended Value: Shows the intended value as configured by Cisco DNA Center.
- Actual Value: Shows the value currently configured on the device.
- Action: Shows **Acknowledge** link for open violations and **Move to Open Violations** link for acknowledged violations.

Do the following to opt-out the violation from the compliance status calculation:

a) Click the **Open Violations** tab.
b) Choose the violation and click **Acknowledge** in the **Actions** column.
c) To acknowledge the violations in bulk, check the check box at the top of the table, or choose multiple violations and click **Acknowledge**.
d) In the confirmation window, click **Confirm**.
The violation is moved to the **Acknowledged Violations** tab.

Do the following to opt-in the violation for the compliance status calculation:

a) Click the **Acknowledged Violations** tab.

b) Choose the violation and click **Move to Open Violations** in the **Actions** column.
c) To move the violations in bulk, check the check box at the top of the table, or choose multiple violations and click **Move to Open Violations**.
d) In the confirmation window, click **Confirm**.
The violation is moved to **Open Violations** tab.

**Step 5** To see a list of attributes that you opted out from the Compliance status calculation, click the **View Preference for Acknowledged Violations** link in **Compliance Summary** window.

**Step 6** In the **Acknowledge Violation Preferences** slide-in pane, do the following to opt-in the attribute for the compliance status calculation:

a) Choose the attribute and click **Unlist** in the **Actions** column.
b) For bulk selection, check the check box at the top of the table, or choose multiple violations and click **Unlist**.

The **Models** tab shows attributes that are acknowledged for Model Config, Routing, Wireless, Application Visibility, or Fabric. Acknowledged templates are shown under the **Templates** tab.

**Note**
- In **Acknowledge Violation Preferences** window, a model with an empty (-) attribute means that the entire model, including its child attributes, are acknowledged.
- When a violation with the status, **Added** or **Removed** is acknowledged, Cisco DNA Center automatically acknowledges similar attributes and their child attributes.
- An acknowledged child attribute cannot be moved to open violations when a similar violation with the status, **Added** or **Removed** is overriding.

# Synchronize Startup and Running Configurations of a Device

When there is a mismatch in the startup and running configurations of a device, you can do a remediation synchronization to match the configurations.

**Step 1** From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

**Step 2** For a bulk remediation, do the following:

a) Choose all the applicable devices.
b) From the **Actions** drop-down list, choose **Compliance** > **Write Running Config to Startup Config**.

For a per-device remediation, do the following:

a) Choose the devices for which you want to do a remediation synchronization.
b) From the **Actions** drop-down list, choose **Compliance** > **Write Running Config to Startup Config**.

Alternatively, click the link under **Compliance** column and then choose **Compliance Summary** > **Startup vs Running Configuration** > **Sync Device Config**.

**Step 3** To view the remedial status of the device, do the following:

a) From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.
b) From the **Actions** drop-down list, choose **Compliance** > **Check Startup Config Write Status**.

# Fix Compliance Violations

Cisco DNA Center allows you to maintain a compliant network by providing an automated fix for device compliance violations. Any deviation from the intent in the device that is identified in the Cisco DNA Center compliance check is fixed with this procedure.

**Step 1** From the top-left corner, click the menu icon and choose **Provision** > **Inventory**.

The compliance column shows the aggregated compliance status of each device.

**Step 2** Click the compliance status to launch the **Compliance Summary** window.

**Step 3** Click **Fix All Configuration Compliance Issues** link, at the top of the window.
The **Fix Configuration Compliance Issues** slide-in pane is displayed.

**Note** The link for fixing compliance violations is visible only if the supported category has violations. Otherwise, the link is not shown.

**Step 4** In **Fix Configuration Compliance Issues** slide-in pane do the following:

a) In the **Summary of Issues to be Fixed** area, review the compliance violations for the network devices. The **Issues Identified** column lists the aggregated count of open and acknowledged violations. Click **Schedule the Fix**.

b) Depending on the Visibility and Control of Configurations settings, choose an available option.

- To immediately deploy the configuration, click **Now**.
- To schedule the deployment for a later date and time, click **Later**, and define the date, time, and time zone of the deployment.
- To preview the configurations, click **Generate configuration preview**.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see Visibility and Control of Configurations Workflow.

c) Edit the default **Task Name**, if required.

d) Click **Apply**.

**Step 5** (Optional) If you chose **Generate configuration preview** in the **Fix Configuration Compliance Issues** slide-in pane, in the **Preview Configuration** window, depending on the Visibility and Control of Configurations settings, do the following:

**a.** Review the device configuration.

**b.** When you're ready, click **Deploy** or **Submit for Approval**. If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**.

**Note** If **Save Intent** displays instead of **Deploy** or **Submit for Approval**, the parameters that you chose during the workflow are already present on the device. To save those parameters to the database, click **Save Intent**. Because no configuration will be pushed to the device, ITSM approval isn't required.

**c.** In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

**d.** Click **Submit**.

**Note** In Cisco DNA Center Release 2.3.7 and later, In IPDT, whenever there is a device role change or protocol endpoint is discovered, and for SNMP trap configuration, if SNMP user group change is detected from the system, intent is updated at Cisco DNA Center side instead of pushing the configuration directly to the device.

**Step 6** On completion of the process, Success message is displayed.

If you previewed and scheduled the task for deployment, you can view the task on the **Tasks** window.

If you submitted the configurations for ITSM approval, you can view the work item's status on the **Work Items** window. If it's not approved, you must resubmit the work item for ITSM approval. When it's approved, it will be deployed at the scheduled time, which you can view on the **Tasks** window.

**Note**
- Routing, Wireless Controller HA Remediation, Software Image, Security Advisories, and Workflow-related compliance issues are not addressed in this fix. You can address these separately by following the actions in their respective sections.
- CLI template compliance has some limitations, because of which some CLI templates may remain noncompliant. For more information, see Limitations in CLI Template Compliance, on page 10.

# Compliance Behavior After Device Upgrade

- A compliance check for all applicable devices (devices for which compliance never ran in the system) is triggered after successful device upgrade.
- Compliance calculates and shows the status of the devices in the inventory, except the Startup vs Running type.
- After upgrade, the Startup vs Running tile shows as NA with the text "Configuration data is not available."
- After a day of successful upgrade, a one-time scheduler runs and makes configuration data available for devices. The Startup vs Running tile starts showing the correct status (Compliant/Noncompliant) and detailed data.
- If any traps are received, the config archive service collects configuration data and the compliance check runs again.

**Note** In the upgrade setup, ignore any compliance mismatch for the **Flex Profile** interface. For the interface name, **1** maps to **management**.

# Limitations in CLI Template Compliance

Cisco DNA Center allows you to compare a CLI template with the running configuration of the device, so as to identify any mismatch from the intent. Note the following comparator engine limitations:

- The CLI Template comparator supports use of uppercase letters for variables and values.

- Avoid using uppercase letters for command keywords.
- The CLI Template comparator supports use of aliases.
- Avoid using abbreviated or shorthand commands, which are flagged as noncompliant.
- If a command is missing and it is at the section level, the section-level commands succeeding the missing command are also flagged. To avoid this problem, use indentation.

  For example, the following CLI Template comparator output shows commands without indentation:

| Realized Template | Running Configuration | Output |
|---|---|---|
| `#interface Vlan111`<br>`#description SVI interface kan-111`<br>`#ip address 111.2.3.4 255.255.255.0`<br>`#ip helper-address 7.7.7.8`<br>`#no mop enabled`<br>`#no mop sysid`<br>`#!` | `#interface Vlan111`<br>`# description SVI interface kan-111`<br>`# ip address 111.2.3.4 255.255.255.0`<br>`# ip helper-address 7.7.7.7`<br>`# ip helper-address 7.7.7.8`<br>`# no mop enabled`<br>`# no mop sysid`<br>`#!` | The following commands are marked as missing:<br><br>`# ip helper-address 7.7.7.7`<br>`# ip helper-address 7.7.7.8`<br>`# no mop enabled`<br>`# no mop sysid` |

The following CLI Template comparator output shows commands with indentation:

| Realized Template | Running Configuration | Output |
|---|---|---|
| `#interface Vlan111`<br>`# description SVI interface kan-111`<br>`# ip address 111.2.3.4 255.255.255.0`<br>`# ip helper-address 7.7.7.8`<br>`# no mop enabled`<br>`# no mop sysid`<br>`#!` | `#interface Vlan111`<br>`# description SVI interface kan-111`<br>`# ip address 111.2.3.4 255.255.255.0`<br>`# ip helper-address 7.7.7.7`<br>`# ip helper-address 7.7.7.8`<br>`# no mop enabled`<br>`# no mop sysid`<br>`#!` | The comparator flags only the missing command:<br><br>`#ip helper-address 7.7.7.7` |

- Interactive and enable mode commands are not compared for compliance. You can use an alternative form of interactive commands by mentioning all the options and values with the commands.

  For example, if the template code is as follows, where **#ENABLE** and **#INTERACTIVE** mode command are given together, the commands are not compared.

```
#MODE_ENABLE
 #INTERACTIVE
    mkdir <IQ>Create directory<R>xyz
 #ENDS_INTERACTIVE
 #MODE_END_ENABLE
#end
```

- Avoid using ranges in commands, which are flagged by the comparator. Ranges must be used in expanded form.
- Overriding commands within the same template are flagged. You can avoid mismatch by enclosing the commands within *ignore - compliance* syntax, as shown in the following example.

| Realized Template | Running Configuration | Output |
|---|---|---|
| `#no banner motd #Welcome to Cisco .:\|:.#`<br>`#banner motd #Welcome to Cisco .:\|:.#` | `#banner motd ^CWelcome to Cisco .:\|:.^C` | • The following command is flagged as missing:<br>`no banner motd #Welcome to Cisco .:\|:.#`<br>• The following command is also marked as missing, because the running command is already compared with the preceding command.<br>`banner motd #Welcome to Cisco .:\|:.#` |

You can do the following to avoid mismatch:

| Realized Template | Running Configuration | Output |
|---|---|---|
| `#! @start-ignore-compliance`<br>`#no banner motd #Welcome to Cisco .:\|:#`<br>`#! @end-ignore-compliance`<br>`#banner motd #Welcome to Cisco .:\|:.#` | `#banner motd ^CWelcome to Cisco .:\|:.^C` | There is no mismatch, because the command enclosed in the syntax is not compared. |

- For later releases of Cisco IOS XE, some default commands are shown only when **show run all** command is issued, instead of the **show run** command. Therefore, these commands do not appear in the running configuration and are flagged as noncompliant.
- Password-bearing commands are flagged by the comparator, because they are stored in encrypted form on the device.

**Note** You can avoid a mismatch for password-bearing commands and some default commands by enclosing the commands in the following syntax:

```
! @start-ignore-compliance
! @end-ignore-compliance
```

Then, reprovision the template for the changes to appear.

To avoid a mismatch between the CLI template and the running configuration of the device, we recommend that you use commands similar to the running configuration.