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 is a weekly compliance check that runs every Saturday at 11:00 pm.

Manual Compliance Run

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

Step 1 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 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 5 minutes to get updated, once traps are received. Hence, we advise you to wait for at least 5 minutes before running Compliance manually after configuration change, to get accurate results.

View Compliance Summary

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

Step 1 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
- Fabric
- Application Visibility

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

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 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** > **Sync Start vs Run Configuration**.

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** > **Sync Start vs Run Configuration**. Alternatively, click the 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) Click the menu icon (☰) and choose **Provision** > **Inventory**.

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

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 5 minutes of any out-of-band changes.	• 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. • Compliant: The startup and running configurations are the same. • NA (Not Applicable): The device, such as AireOS, is not supported for this compliance type.

Compliance Type	Compliance Check	Compliance Status
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. • Compliant: The device is running the tagged golden image of the device family. • NA (Not Applicable): The golden image is not available for the selected device family.
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. • Compliant: There are no critical vulnerabilities in the device. • 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. **Note** Network profile compliance is applicable for routers, switches and wireless controllers.	• Noncompliant: The device is not running the intent configuration of the profile. • 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. • Error: The compliance could not compute the status because of an underlying error. For details, see the error log.
Fabric (SDA) This feature is in beta.	Fabric compliance helps to identify fabric intent violations, such as any out-of-band changes for fabric-related configurations.	• Noncompliant: The device is not running the intent configuration. • 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. 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. • Compliant: The intent configuration of CBAR/NBAR is running on the device.

Compliance Type	Compliance Check	Compliance Status
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. • Compliant: The attributes in Model Config match the intended value.
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. 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 5 minutes to get updated, once traps are received. Hence, we advise you to wait for at least 5 minutes before running Compliance manually after configuration change, to get accurate results. **Note** There are some limitations in CLI template compliance. See Limitations in CLI Template Compliance, on page 6.	• Noncompliant: There is mismatch between the CLI template and the running configuration of the device. • Compliant: There is no mismatch between the CLI template and the running configuration of the device.

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.

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 section level, the section level commands succeeding the missing command are also flagged. By giving indentation the problem can be avoided.

  For example,

  Cli template comparator output, for commands without indentation:

Realized Template	Running Configuration	Output

`#interface Vlan111`
`#description SVI interface kan-111`
`#ip address 111.2.3.4 255.255.255.0`
`#ip helper-address 7.7.7.8`
`#no mop enabled`
`#no mop sysid`
`#!`
	`#interface Vlan111`
	`# description SVI interface kan-111`
	`# ip address 111.2.3.4 255.255.255.0`
	`# ip helper-address 7.7.7.7`
	`# ip helper-address 7.7.7.8`
	`# no mop enabled`
	`# no mop sysid`
	`#!`
		The below commands are marked as missing:
		`# ip helper-address 7.7.7.7`
		`# ip helper-address 7.7.7.8`
		`# no mop enabled`
		`# no mop sysid`

  Cli template comparator output, for commands with indentation:

Realized Template	Running Configuration	Output

`#interface Vlan111`
`# description SVI interface kan-111`
`# ip address 111.2.3.4 255.255.255.0`
`# ip helper-address 7.7.7.8`
`# no mop enabled`
`# no mop sysid`
`#!`
	`#interface Vlan111`
	`# description SVI interface kan-111`
	`# ip address 111.2.3.4 255.255.255.0`
	`# ip helper-address 7.7.7.7`
	`# ip helper-address 7.7.7.8`
	`# no mop enabled`
	`# no mop sysid`
	`#!`
		Only missing command is flagged by the comparator:
		`#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 below.

  For example,

Realized Template	Running Configuration	Output

`#no banner motd #Welcome to Cisco .:|:.#`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	• The below commands is flagged as missing:
		`no banner motd #Welcome to Cisco .:|:.#`
		• The below command is also marked as missing, as the running command is already compared with the above command.
		`banner motd #Welcome to Cisco .:|:.#`

  You can do the following to avoid mismatch:

Realized Template	Running Configuration	Output

`#! @start-ignore-compliance`
`#no banner motd #Welcome to Cisco .:|:#`
`#! @end-ignore-compliance`
`#banner motd #Welcome to Cisco .:|:.#`
	`#banner motd ^CWelcome to Cisco .:|:.^C`	No mismatch as the command enclosed in the systax 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 device, we recommend that you use commands similar to the running configuration.