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 that do not meet compliance requirement for the different aspects of compliance such as Software Image, PSIRT, Network Profile and so on in Cisco DNA Center.

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 notification from various services such as inventory, SWIM, and so on to assess data.
- Manual compliance check: Enables user to 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 pm.

Manual Compliance Run

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

Step 1 In the Cisco DNA Center GUI, 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 on compliance column (if available) and then click on **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.

View Compliance Summary

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

Step 1 In the Cisco DNA Center GUI, 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.

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, then 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 five minutes of any **out of band** changes.	• Noncompliant: The Startup and Running configuration are not the same. On detail view, the system shows different startup versus running between or running versus previous running. • Compliant: Startup and Running Configuration are the same. • NA (Not Applicable): The device is not supported for this compliance type (for example, AireOS).
Software Image	This compliance check helps network administrator to see if tagged golden image in Cisco DNA Center is running on the device or not. It shows the difference in golden image and 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)	PSIRT Compliance check enables the network administrator in checking whether the network devices are running without any critical security vulnerabilities or not.	• 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 network administrator in Cisco DNA Center or the device is not supported.
Network Profile	Cisco DNA Center allows you to define its intent configuration via Network Profile and pushes to device via provisioning. The Intent must be running on a device. If any violations are found at any time due to **out of band changes**, compliance identify, assess and flag it off. The violations are shown to the user under **Network Profiles** on the compliance summary page. The automatic compliance check is scheduled to run after a period of 5 hours. **Note** Network profile compliance is only applicable for routers and wireless LAN controllers and not for switches.	• Noncompliant: The device is not running the intent configuration of profile. • Compliant: The intent configurations are running on the device. • Error: The compliance could not compute status because of an underlying error. For more details, please refer to the error log.
Fabric (SDA Profile)	Fabric compliance helps to identify the 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 application visibility intent and provision it to devices via CBAR and NBAR. If there is an intent violation on devices, compliance identity, assess, and show the violaion as compliant or noncompliant under **Application Visibility**. The automatic compliance check is scheduled to run after a period of 5 hours.	• Noncompliant: The CBAR/NBAR configuration is not running on the device. • Compliant: The intent configuration of CBAR/NBAR is running on the device.

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**.