Cisco Catalyst Center Base Automation Services Troubleshooting Guide

Revised: April 8, 2024,

Troubleshooting Base Automation Services

This guide provides troubleshooting information for the base automation services in Catalyst Center. For further assistance on any of the issues, contact customer support.

Compliance Service Troubleshooting

This section provides troubleshooting information for common compliance-related issues.

General Checklist

- Ensure that the device is reachable so that it can trigger compliance check and read the latest compliance check status.
- Ensure that the device is part of the supported device family.
- Ensure that previous compliance checks are complete before triggering a new compliance check.
- Ensure that the device supports compliance checks. The support for various compliance checks depends on the intent configured and deployed on the device.
- Ensure that the device can send events, such as SNMP, syslog, and so on, to support event-based automatic compliance check and Config Drift.
- Ensure that you have admin privileges to run, acknowledge, and fix compliance violations.

Basic Troubleshooting

The following table provides troubleshooting information for some common compliance-related issues in the device inventory.

Issue	Possible Cause and Solution
The compliance status shows as *In Progress* for a long time.	It means that the compliance check is either waiting or running. This can be due to any of the following reasons: • A provisioning task that's in progress; compliance checks have lower priority and wait for provisioning to complete. • Compliance checks may need to wait up to 24 hours when there are higher priority tasks. • A user-triggered compliance check has higher priority than a system-triggered compliance check. Wait for the compliance check to complete. If the status is *In Progress* for more than seven days, the task is automatically canceled, and the compliance check is retriggered.

Issue	Possible Cause and Solution
The compliance status is in *Error* state.	When any one of the compliance checks is in the error state, the overall compliance status displays *Error*. Click the info icon to see the error message or check the compliance summary to see the compliance which is causing the error. You can trigger a manual compliance check to see if the issue is intermittent. If the issue persists, contact customer support.
The compliance status is in *Aborted* state.	It means that compliance which were in progress for more than seven days have been canceled. After canceling, compliance checks are retriggered automatically; user intervention is not required.
The compliance status is *NA* (Not Available or Not Applicable).	Check if the devices support compliance service and have the required licensing. The following device families do not support compliance service: • Security and VPN • Cisco Enterprise Network Functions Virtualization Infrastructure Software (NFVIS) • Content networking • Wireless sensor • Meraki dashboard • Meraki switches • Meraki security appliances
Unable to trigger compliance checks from inventory.	This option is disabled for devices that are unreachable or unsupported. Choose devices that are supported and reachable.

Issues in Compliance Summary

The **Compliance Summary** pane displays compliance check tiles such as, **Startup vs Running Configuration**, **EoX - End of Life**, and **Software Image**.

Startup vs Running Configuration

The following table provides troubleshooting information for **Startup vs Running Configuration** compliance checks.

Issue	Possible Cause and Solution
The status is showing as NA (Not Applicable).	The status is shown as NA when either startup or running configuration is missing in the latest device archive. If the device supports both startup and running configuration, this issue is resolved automatically in the next event-driven archive.

Issue	Possible Cause and Solution
The status is showing as compliant when it's expected to be noncompliant.	The running configuration is a collection of the **show running config** command and hence, doesn't include default commands. Some of the device autogenerated commands are also ignored from the running configuration so that the device doesn't show as noncompliant every time it reloads.
The status is outdated or not updated frequently.	This check is based on the Config Drift feature. Configure Catalyst Center as the syslog server in the **Design** > **Network Settings** > **Telemetry** window. Ensure that the device is able to send syslogs to Catalyst Center.
The status is showing as noncompliant when it's expected to be compliant.	This issue can occur if any configuration is either pushed from Catalyst Center without selecting the **copy startup to running config** option or directly configured on the device without configuring the **write memory** or **copy running-config startup-config** option. To manually fix the issue, use the **Sync Device config** option in the tile or use the **Fix All Compliance Configuration Issues** option (supported in Catalyst Center Release 2.3.5 and later).
Can violations be acknowledged?	Violations under this category cannot be acknowledged.
Can violations be remediated?	Violations can be remediated using any one of the following options: • **Sync Device config** in the tile. • **Fix All Compliance Configuration Issues** in the compliance summary window. • **Write Running Config to Startup Config** under **Actions** > **Compliance** in the **Inventory** window.
How long does it take to update the **Startup vs Running Configuration** tile automatically?	The tile is updated when a config drift is collected. However, collecting a config drift has a cool down period from the time of the last config change syslog. If a new config change syslog is received within this cool down period, the cool down timer restarts. The drift data is collected and updated at the regular compliance schedule as well, which is five hours after the first config change notification from inventory. You can see the schedule in the compliance summary window.

Issue	Possible Cause and Solution
How do you trigger a manual compliance check for this tile?	Click **Run Compliance Check** in the compliance summary window. To trigger bulk checks, in the **Inventory** window, select the devices. Then, from the **Actions** drop-down list, choose **Compliance** > **Run Compliance Check**. This compliance check uses the Config Drift feature (which is not triggered by running a compliance check) and unless a new config drift is generated, running a manual check uses the same latest config drift every time, giving the same result.

EoX - End of Life

The following table provides troubleshooting information for **EoX - End of Life** compliance checks.

Issue	Possible Cause and Solution
The tile is missing in the compliance summary window.	This is a static tile that appears for all devices in Catalyst Center Release 2.3.4 and later.
The status is showing as NA (Not Applicable).	This check requires the user's consent to connect to CX cloud and have the EoX data available in the inventory.
Can violations be acknowledged?	Violations under this category cannot be acknowledged.
Can violations be remediated?	Violations under this category cannot be remediated.
How long does it take to update the **EoX - End of Life** tile automatically?	This tile is updated when there's new data from a security advisory scan. This tile is updated at the regular compliance schedule as well, which is five hours after the first configuration change notification from inventory. You can see the schedule in the compliance summary window. A regular update uses the latest available security scan data and doesn't trigger a new scan.
How to trigger a manual compliance check for this tile?	Click **Run Compliance Check** in the compliance summary window. To trigger bulk checks, in the **Inventory** window, select the devices. Then, from the **Actions** drop-down list, choose **Compliance** > **Run Compliance Check**. This compliance check depends on the security advisory scan which occurs periodically when it is enabled in the **System** > **Settings** > **Machine Reasoning Engine** window under **Security Advisory Settings**. You can check the security scan task details on the **Activities** > **Tasks** window.

Software Image

The following table provides troubleshooting information for **Software Image** compliance checks.

Issue	Possible Cause and Solution
Is the **Software Image** tile applicable for my device?	This is a static tile that appears for all devices.
The status is showing as NA (Not Applicable).	For nonstack devices, you need to mark a golden image version in the **Design** > **Image Repository** window.
The status is showing as noncompliant even when there's no marked golden image.	For stack devices, this tile highlights the version mismatch between primary and other stack members even when there's no marked golden image. When a golden image is marked for the device, all stack members must be on that version for the device to be compliant.
The status is showing as compliant even when there's no marked golden image.	For stack devices, this tile shows the version mismatch between primary and other stack members.
Can violations be acknowledged?	Violations under this category cannot be acknowledged.
Can violations be remediated?	Violations under this category cannot be remediated from compliance but can be remediated using the image update workflow.
How long does it take to update the **Software Image** tile automatically?	This tile is updated when there's a change in the image or marking of golden image. This tile is updated at the regular compliance schedule as well, which is five hours after the first configuration change notification from inventory. You can see the schedule in the compliance summary window. For regular updates, information from the image repository (SWIM) is used.
How to trigger a manual compliance check for this tile?	Click **Run Compliance Check** in the compliance summary window. To trigger bulk checks, in the **Inventory** window, select the devices. Then, from the **Actions** drop-down list, choose **Compliance** > **Run Compliance Check**. This compliance check uses data from the SWIM service and fresh data is fetched every time a compliance check is triggered.

Network Settings

The following table provides troubleshooting information for **Network Settings** compliance checks.

Issue	Possible Cause and Solution
The tile is missing in the compliance summary window.	This is a static tile that appears for all devices in Catalyst Center Release 2.3.5 and later.
The status is showing as NA (Not Applicable).	The status is shown as NA until the device is assigned to a site or provisioned. The status is updated when the compliance check runs after assigning a site or provisioning.
Is it required to run a compliance check after an upgrade?	A compliance check is scheduled to run automatically five hours post upgrade; user intervention is not required.

Issue	Possible Cause and Solution
Can violations be acknowledged?	Violations under this category can be acknowledged. Similar violations are acknowledged automatically.
Can violations be remediated?	Violations under this category can be remediated using the **Fix All Configuration Compliance Issues** option.
How long does it take to update the **Network Settings** tile automatically?	This tile is updated at the regular compliance schedule, which is five hours after the first configuration change notification from inventory. You can see the schedule in the compliance summary window.
How to trigger a manual compliance check for this tile?	Click **Run Compliance Check** in the compliance summary window. To trigger bulk checks, in the **Inventory** window, select the devices. Then, from the **Actions** drop-down list, choose **Compliance** > **Run Compliance Check**. This compliance check depends on the manageability status of the device. Make sure to sync the device either manually or automatically before triggering the compliance check to get accurate and updated results.

Network Profiles

The following table provides troubleshooting information for **Network Profiles** compliance checks.

Issue	Possible Cause and Solution
This tile is missing in the compliance summary window.	This is a dynamic tile that appears for devices provisioned with a network profile. The tile appears during the first compliance check after the device is provisioned.
Can violations be acknowledged?	Violations under this category can be acknowledged. Similar violations are acknowledged automatically.
Can violations be remediated?	Violations under this category can be remediated using the **Fix All Configuration Compliance Issues** option except for routing violations.
The violations seem inaccurate.	The violations may seem inaccurate due to any of the following reasons: • Compliance check is not completed and might be scheduled for the device. You can check the schedule in the compliance summary. • The device is either in an unmanaged state or not in sync. Ensure that the device is in managed state and in sync (event-triggered sync or automatic inventory sync). You can resync manually using the **Actions** > **Resync** option in the **Inventory** window. Run the compliance check manually after config drift data collection to get accurate results.

Issue	Possible Cause and Solution
The template compliance violation isn't visible.	Template compliance is available in Catalyst Center Release 2.3.3 and later. Templates must be attached and deployed via a network profile. Template compliance is checked during the first compliance check after provisioning.
Template compliance violations are always present.	Template compliance has limitations; check if these are considered during template design. If not, correct and redeploy the committed template. Use ignore tags if required.
Template compliance violations are not updating.	Template compliance uses the running configuration collected by the syslog event-based config drift. Before running the compliance check manually, ensure that Catalyst Center is configured as a syslog server in the **Design** > **Network Settings** > **Telemetry** window and the latest device archive contains the changes.
How to check which templates are being compared (both compliant and noncompliant)?	Contact customer support for assistance.
How long does it take to update the **Network Profiles** tile automatically?	This tile is updated at the regular compliance schedule, which is five hours after the first configuration change notification from inventory. You can see the schedule in the compliance summary window.
How to trigger a manual compliance check for this tile?	Click **Run Compliance Check** in the compliance summary window. To trigger bulk checks, in the **Inventory** window, select the devices. Then, from the **Actions** drop-down list, choose **Compliance** > **Run Compliance Check**. This compliance check depends on the manageability status of the device. Make sure to sync the device either manually or automatically before triggering the compliance check to get accurate and updated results. Also, check the above issue: *Template compliance violations are not updating*.
What are the additional data that can be collected while filing a bug?	When raising a template compliance bug, attach a screenshot of the realized template and text file of the running configuration to check if the event-based config drift is working as expected.

Fabric, Application Visibility, Cisco Umbrella, and Workflow

The following table provides troubleshooting information for **Fabric, Application Visibility, Cisco Umbrella, and Workflow** compliance checks.

Issue	Possible Cause and Solution
The tile is missing in the compliance summary window.	These are dynamic tiles that appear only for devices that have the required configurations enabled and provisioned.
Can violations be acknowledged?	Violations under this category can be acknowledged. Similar violations are acknowledged automatically.

Issue	Possible Cause and Solution
Can violations be remediated?	Violations under this category can be remediated using the **Fix All Configuration Compliance Issues** option except for Site to Site VPN violation under the **Workflow** tile.
How long does it take to update the tiles automatically?	The tiles are updated at the regular compliance schedule, which is five hours after the first configuration change notification from inventory. You can see the schedule in the compliance summary window.
How to trigger the manual compliance check for these tiles?	Click **Run Compliance Check** in the compliance summary window. To trigger bulk checks, in the **Inventory** window, select the devices. Then, from the **Actions** drop-down list, choose **Compliance** > **Run Compliance Check**. This compliance check depends on the manageability status of the device. Make sure to sync the device either manually or automatically before triggering the compliance check to get accurate and updated results.
The device is shown as compliant in inventory, but the fabric status is noncompliant in the compliance summary.	The fabric compliance feature is in the beta phase. Hence, fabric status is not considered in the overall device compliance.

Issues in Acknowledge Compliance

The Acknowledge Compliance feature allows you to acknowledge compliance violations that are less important and ignore these violations from the overall compliance status calculation. The following table provides troubleshooting information for some common issues in the Acknowledge Compliance feature.

Issue	Possible Cause and Solution
This option isn't visible.	The Acknowledge Compliance feature is available in Catalyst Center Release 2.3.4 and later. The feature doesn't require any enabling. From the compliance summary window, click any of the compliance tiles that has violations and choose the required action in the **Open Violations** or **Acknowledged Violations** tab.
What violations can be acknowledged?	You can acknowledge only Catalyst Center intent violations, that is, violations under **Network Settings**, **Network Profiles**, **Fabric**, **Application Visibility**, **Cisco Umbrella**, and **Workflow**.
Does an acknowledged violation need to be reacknowledged when the compliance check runs again?	After a violation is acknowledged, it remains acknowledged until it is removed manually from the acknowledged list. The status isn't impacted by multiple compliance runs, the absence of a violation or reappearance of a violation.
How do you view all the acknowledged models and attributes?	Use the **View Preference for Acknowledged Violations** option in the compliance summary window or the compliance tile to view the acknowledged models and attributes for a device.

Issue	Possible Cause and Solution
What does a "—" in the attribute column mean in the **List of Acknowledged Violation Attributes** table?	A model with an empty attribute ("—") means that the entire model including its child attributes is acknowledged and all violations under the same model or its child attributes are acknowledged automatically.
Why are all similar violations automatically acknowledged or moved to open violations even when only one violation is selected?	The Acknowledge Compliance feature considers models and attributes (for example, WLAN configuration is a model containing attributes such as, broadcast SSID, admin status, and so on) rather than values to retain the acknowledgment status through multiple compliance runs or value changes. At a given time, a violation could be due to *Value 1* and at another time due to *Value 2*. The violation should remain acknowledged for both of these. For example: • When a violation with the *Removed* or *Added* status is acknowledged, all violations of its child attributes and any future *Removed*, *Added*, or *Changed* type of violations are automatically acknowledged. Similar logic is followed for **Move to Open Violations**. • When a violation with the *Changed* status is acknowledged, all violations with the same model and attribute and any future violations with the same model and attribute are automatically acknowledged. If there is a violation with the *Removed* or *Added* status, the violations are not acknowledged automatically. Similar logic is followed for **Move to Open Violations**. Automatic acknowledgment is not applicable for CLI templates.

Issue	Possible Cause and Solution
After acknowledging multiple violations, the **List of Acknowledged Violation Attributes** table shows only a few acknowledged violations.	The **List of Acknowledged Violation Attributes** table lists only the models and the corresponding attributes that have been acknowledged, it does not list all the violations that correspond to the model. For example, if the WLAN model with broadcast SSID attribute has four violations due to four different SSIDs, acknowledging the four violations would create only one entry indicating the model is WLAN and the attribute is broadcast SSID. There are no duplicate entries. When a removed or added type of violation is acknowledged for WLAN, then only one entry would appear in the **List of Acknowledged Violation Attributes** table, indicating the WLAN model with the attribute "—" (which means all attributes including the child models and attributes) is acknowledged. In this case, previously acknowledged attribute entries (which in this example means, the model is WLAN and the attribute is broadcast SSID) are removed and only this entry remains. This indicates that acknowledgments of added or removed type of violations take precedence over changed type of violations.
Cannot move acknowledged violations to open violations.	Acknowledgments of added or removed type of violations take precedence over changed type of violations. If you try to move a violation to open violations for a child attribute of a model when there are existing added or removed type of violations for the same model, an error is shown. You can either move all violations to open violations or leave them as acknowledged.
How do you move acknowledged violations that are no longer present?	Use the unlist option in the **List of Acknowledged Violation Attributes** table.

Issues in Fix Compliance

Catalyst Center provides an option to fix the device compliance violations in the compliance summary window. The following table provides troubleshooting information for some common issues while using the Fix Configuration Compliance Issues feature.

Issue	Possible Cause and Solution
This option isn't available.	This option is available in Catalyst Center Release 2.3.5 and later. The feature doesn't require any enabling. The **Fix All Configuration Compliance Issues** option is displayed in the compliance summary window when there are violations that can be remediated.
What violations can be fixed?	You can fix only the supported Catalyst Center intent violations. Violations under Routing, Wireless Controller High Availability, Software Image, Securities Advisories, and Workflow are not supported.

Issue	Possible Cause and Solution
When a mobility or guest anchor is configured, will this option fix all devices?	In these cases, the violations are not fixed automatically on all such devices. A notification is displayed for such scenarios. A network flap might occur if only one device is remediated. Make sure to generate a preview configuration and review it before pushing it to the device.
Is there any action required to see the updated compliance status after completing the remediation?	As a part of the remediation workflow, the automatic config drift collection and compliance checks are triggered. There is no need to resync or wait for the config archive or trigger the compliance check manually.
The compliance status in noncompliant even after completing remediation.	Check if you have conflicting intent in your profiles. For example, if there's a template that is overriding the intent in the network profile, the status shows as noncompliant; configure the intent correctly and reprovision the device. If there are template compliance violations arising due to template limitations, follow the workarounds for these limitations or use the acknowledge feature for less important violations.
How do you view the remediation task details?	You can see the remediation task details on the **Tasks** window. To navigate to the **Tasks** window, click the menu icon and choose **Activities** > **Tasks**. Filter the category as **Compliance Remediation** and select the task.
What happens if a device becomes compliant when a remediation is scheduled?	Prechecks are run before initiating the remediation workflow. In this case, because the prechecks fail, the remediation task also fails indicating that there are no violations to be remediated.
What happens if a device becomes compliant when the deployment is scheduled after previewing remediation commands?	The commands generated in the preview configuration are considered where the optimization skips the already present commands. The device remains compliant and the config drift is collected if not collected already. If the config drift is present with the latest changes, the optimization logic in config drift does not save the new archive.
What happens if more violations appear when a remediation is scheduled?	The remediation workflow considers all the supported violations and fixes the issues.
What happens if more violations appear when the deployment is scheduled after previewing remediation commands?	Only the commands generated in the preview configurations are considered and pushed to the device which results in partial remediation and the device shows as noncompliant even after successful remediation.
What additional data can be collected while filing a bug?	You can collect the following data while filing a bug: • SPF service logs. Enable the debug mode while collecting logs, if possible. • Screen captures of violations and database dumps.

Config Archive Service Troubleshooting

This section provides troubleshooting information for the config-archive service.

General Checklist

System

- Ensure that you have write access to compliance and network provision to perform **Sync Device Config** and **Write Running Config to Startup Config** operations.
- Ensure that Catalyst Center is configured as a syslog server and SNMP trap server (For AireOS devices) under **Design** > **Network Settings** > **Telemetry**.

Device

- Ensure that the device is reachable to collect configurations or to perform the **Write Running Config to Startup Config** operation.
- Ensure that the device is part of the supported device family.
- Ensure that the device is assigned to a site or is in a provisioned state, so that it can send syslog events (or SNMP events for AireOS) for the event-based automatic config drift to work.

Basic Troubleshooting

The following table provides troubleshooting information for some common issues in the config archive service.

Issue	Possible Cause and Solution
How to check if the syslog event-based archive is working?	You can follow the below steps to test the event-based archiving: **1.** Before you begin, ensure the following: • Catalyst Center is configured as syslog server under **Design** > **Network Settings** > **Telemetry**. • The device is assigned to a site and provisioned. • The device has the Catalyst Center IP or FQDN configured as the logging host. To check, use the **show running-config | include logging** command. **2.** Choose a supported device to test the event-based archive. Check the latest configuration changes under the **Config Drift** tab in device details. **3.** Log in to the device terminal and make any simple configuration change, such as the banner. **4.** Log out of the device terminal and make sure that there are no other configuration processes running. Note the time at this point. **5.** Wait for at least five minutes after the noted time and then check the **Config Drift** tab under device details. Refresh the window, if needed. The window displays the new configuration changes. **6.** Revert the changes made in Step 3. A new event is triggered and an archive is collected after a cool down period.

Issue	Possible Cause and Solution
How to check if the SNMP trap-based archive is working for AireOS devices?	You can follow the below steps to test the SNMP trap-based archiving: **1.** Before you begin, ensure the following: • Catalyst Center is configured as an SNMP server under **Design** > **Network Settings** > **Telemetry** • The device is assigned to a site and provisioned. • The device has the Catalyst Center IP or FQDN configured as an SNMP server. To check, use the **show running-config** command and check for **snmp trapreceiver** configuration. **2.** Choose a supported device to test the event-based archive. Check the latest configuration changes under the **Config Drift** tab in device details. **3.** Log in to the device terminal and make any simple configuration change, such as *config logging syslog level warning*. **4.** Log out of the device terminal and make sure that there are no other configuration process running. Note the time at this point. **5.** Wait for at least five minutes after the noted time and then check the **Config Drift** tab under device details. Refresh the window, if needed. The window displays the new configuration changes. **6.** Revert the changes made in Step 3. A new event is triggered and an archive is collected after a cool down period.
Why isn't the archive collected? How long does it take to automatically collect an archive?	A configuration archive collection could be delayed when there are frequent configuration changes and the device is sending configuration change syslogs continuously, which results in an extended cool down period. The archive collection starts five minutes after the last configuration change syslog. Ensure that there are no frequent configuration changes on the device. The opening and closing of a device configure terminal can also generate configuration change syslogs. To check if the syslog events from the device are reaching the config archive service, see *How to check if syslog event-based archive is working?*

Issue	Possible Cause and Solution
Why isn't the drift point visible in the timeline? Why is the weekly archive not visible?	When a latest archive contains the same information as the previous archive, the latest archive is discarded to save disk space. Hence, there is no drift point visible on the timeline. This logic applies to the weekly archive also. To check if the event-based archive is working or not working, see *How to check if syslog event-based archive is working?* In Catalyst Center Release 2.3.7 and later, the config drift window displays the last updated time. If the latest drift point on the timeline has an older timestamp than the last updated time, it means that there are no configuration changes since the latest drift point.
The config drift window is displaying the "approaching storage limit" warning.	This warning appears when the number of labeled configurations has reached 80% of the maximum number of archives to be stored per device. You can try removing the labels of older config drifts or increase the total number of config drifts per device—minimum 7 and maximum 50 config drifts; increasing the number increases the disk utilization.
The external SFTP server cannot be added.	You can perform the following checks while adding the SFTP server: • Check the parameters while adding the servers. Not all third-party SFTP servers are supported. • Ensure that the directory of the root location is empty. • Ensure that the root location path is absolute. • If you have a backup in *raw* format that is not working, try with a *sanitized* format. If both formats are not working or *sanitized* is working but not raw, collect the logs and contact customer support.
The files on the external SFTP server are empty.	When the task of copying files to an external SFTP server is successful but the files on the server are empty, check the available free memory in the root location on the server. A lack of memory causes this problem. Try to increase the memory and copy the files. If the problem persists, contact customer support.

Inventory Services Troubleshooting

The following sections provide troubleshooting information for the inventory service, event service, and the network design service.

Inventory Service

Issue	Possible Cause and Solution
How to check if the inventory service is working?	Check if the discovery jobs that were created earlier are displayed in the Catalyst Center **Discovery** window and if the devices that were added or discovered earlier are displayed in the Catalyst Center inventory. If there is no data in the inventory, do the following: **1.** Ensure that the **ncp-node** and **inventory** services are up and running. **2.** If the services are up and running, check the device count by running the **Get Device Count** API under the Catalyst Center developer kit (**Help** > **Developer Resources**). If the API call returns the device count, it ensures that the inventory service is working and the problem could be a localized GUI issue. For further assistance, contact customer support.
Device addition or device update issues.	While adding or updating a device, ensure the following: • Ensure that the device is added with the correct CLI credentials. Otherwise, the device shows a CLI authentication error in the **Inventory** window. • Ensure that SNMP credentials are working. The SNMP authentication error or SNMP timeout error can be due to incorrect SNMP credentials or connectivity issues. After adding the device, Catalyst Center connects to the device based on the credentials given. If there are any errors while connecting to the device, it is shown in the **Manageability** status column in the **Inventory** window. Hover over the error icon for more information about the error and possible solutions. For further assistance, contact customer support.

Issue	Possible Cause and Solution
Device resynchronization issues.	Ensure the following: • Ensure that the device is added with the correct CLI credentials. Otherwise, the device shows a CLI authentication error in the **Inventory** window. • Ensure that SNMP credentials are working. The SNMP authentication error or SNMP timeout error can be due to incorrect SNMP credentials or connectivity issues. If there are any errors during device resync, it is shown in the **Manageability** status column in the **Inventory** window. Hover over the error icon for more information about the error and possible solutions. For further assistance, contact customer support. **Note** Device resynchronization is triggered after the inventory service restart under the following circumstances: • If there is an upgrade (Catalyst Center upgrade) after the inventory service restart. • If the device's synchronization is in terminated or delayed state after the service restart. • If the **Last Sync** time for the device is more than 75 percent of the periodic resync interval configured on the device. For example, after the inventory service restart, if the **Last Sync** time for a device has crossed 18 hours and the configured periodic resync interval is 24 hours, the device will be resynchronized before the periodic resync interval. The percentage for the resync interval cutoff time may vary based on the value configured on the device.
Device deletion issues.	Device deletion with configuration cleanup involves the deletion of device controllability and other telemetry-related configurations. Device deletion fails when any of the associated configurations are not deleted. Error messages displayed in the Catalyst Center GUI show the tasks that have failed. If there are any database-related exceptions or errors, contact customer support.

Device Discovery Issues

Issue	Possible Cause and Solution
Discovery page is not loading.	Check if the **apic-em-inventory-manager-service** is up and running.

Issue	**Possible Cause and Solution**
Cannot start a discovery.	When you start a discovery and see the error message, *"An invalid response was received from the backend service. Please refer to the backend service logs for more details"*, check if the **scheduler-service** is up and running.
The discovery task is in the queued or scheduled state for a long time.	Perform the following checks: • Filter the discovery job by the *in progress* status and check if there is any discovery in progress. Discovery jobs are queued and run one at a time. • Check if there are any discoveries starting with EN-discovery. These discoveries are triggered automatically to discover unreachable extended nodes. Check the unreachable nodes and fix the reachability issues for such devices. If the devices are not being used, try deleting them. This helps in reducing the number of autotriggered discoveries.
Changes made in global credentials are not seen during the discovery.	Retriggering an existing discovery considers the old credentials with which the discovery was done initially. Start a new discovery after editing global credentials.
Cisco Discovery Protocol (CDP) and Link Layer Discovery Protocol (LLDP) discoveries are taking a long time.	Perform the following checks: • Check the hop count in **CDP Level** and **LLDP Level**. A higher hop count results in longer discovery time. • Check if there are more unreachable devices listed as CDP and LLDP neighbor. • Check the number of credentials for the discovery job. Multiple credentials can lead to a longer validation time.
The device is discovered with a different IP address, which is out of the IP address range entered during discovery.	If a device being discovered is already available in the inventory, it is discovered with the existing IP address.
Discovery is complete, but the results don't show any devices.	Check if any of the IP addresses given in the IP address range are reachable through a ping test. Only the devices that are reachable through the ping test are listed in the discovery results.

Event Service

Issue	Possible Cause and Solution
How to check the sync status during an event?	You can check the sync status for an event by triggering a trap scenario and observing the sync details in the device inventory. If the sync is due to the trap, a corresponding reason can be seen in the sync details. There can be multiple sync requests at a given time. The following sync reasons are displayed based on the event that triggered the sync: • AP event • Config change event • Link up/down event • Redundancy event

Network Design Service

Issue	Possible Cause and Solution
Configuration not pushed to the device.	Verify the configuration pushed to the device during provisioning: • Check the syslog configurations that are pushed in the provision summary. • Check the device audit logs to see the syslog configurations that are pushed to the device. Check the errors that are displayed when the CLI configuration push fails: • CLI authentication error: This occurs when the device is unreachable through the credentials provided in Catalyst Center. Check the reachability of the device and push the configuration again using the retry option. • Max length reached: This error is related to the syslog configuration push and occurs when the maximum configuration limit is reached on the device. For example, *"Unable to add 10.0.0.1 to syslog host list. Maximum number of hosts already configured"*. Remove the unused configurations from the device and retry the configuration push. • Invalid CLI: This occurs when the device does not support CLI configuration due to either insufficient permissions to configure the CLI or lack of support for the configurations on the device. If the configurations are not supported on the device, contact customer support for further assistance. • Device timeout: This occurs due to an improper handling of an interactive command during a configuration push. Contact customer support for further assistance.

Issue	Possible Cause and Solution
A compliance error is displayed.	Perform the following checks: • You can check the syslog, SNMP, IP Device Tracking (IPDT), and Cisco TrustSec (CTS) configuration issues under the **Network Settings** compliance tile in the **Compliance Summary** window. For more information about the intended value for the configuration, click **View details** under the **Intended Value** column. • To identify if the intent is correct or not, check the audit logs for the last command push related to the compliance error. • Use the remediation workflow in the **Compliance** window to fix the compliance issues.
The configuration isn't supported by the device.	When the configuration is not supported by the device, the configuration push is filtered out, and an error message is shown in the provisioning summary.
Cisco ISE integration and CTS push errors are displayed.	Check the errors that are displayed: • Overlapping IP address: This error occurs when Cisco ISE already has a device with the same IP address as the one that you're trying to push to Cisco ISE. Remove the device entry from Cisco ISE and retrigger the provisioning. • The device ID is not unique: This error occurs when Cisco ISE already has a device with the same serial number as the one that you're trying to push to Cisco ISE. Remove the device entry from Cisco ISE and retrigger the provisioning. • CTS deployment error: Check if a Cisco ISE Network Access Device (NAD) entry is created for the device you're provisioning because CTS is pushed only after a NAD entry is created. Check if the device is applicable for the CTS configuration. For further assistance, contact customer support. • Mandatory field requirements error: Cisco ISE requires a few mandatory fields for the NAD entry creation. Depending on the Cisco ISE versions, these fields might differ and in the event of a missing mandatory field, the NAD entry creation might fail. For further assistance, contact support. • CTS push failure due to CLI authentication error: In this case, provisioning fails due to the error and a retry option is provided. Correct the device CLI credentials and retry.
IPDT configuration issues.	If the IPDT settings are not pushed to certain interfaces, check if the interfaces fall into the excluded list. The following interfaces are excluded for IPDT configuration: • Interfaces configured with switchport mode trunk. • Interfaces connected to neighbors or other network devices. • Interfaces connected to *lagEndport* and the operation state is down. • StackWise Virtual ports and StackWise Virtual Dual-Active Detection (DAD) ports. • Interface names that start with *Bluetooth*, *AppGigabitEthernet*, and *Port*.

Licensing Service Troubleshooting

The following table provides troubleshooting information for some common issues in the licensing service.

Issue	**Possible Cause and Solution**
How to enable the debug logs for licensing service?	From the top-left corner, click the menu icon and choose **System** > **Settings** > **Debugging Logs**. Then enable the debugging logs for the **licensemanager** service.
NETCONF connectivity issues.	Ensure the following: • The device has NETCONF enabled with the correct NETCONF port. • The device is in a managed state without any NETCONF connectivity failures.
Smart Licensing Using Policy (SLP) workflow issues.	For issues in the license management reporting workflow, perform the following checks: • Ensure that the device has NETCONF enabled with the correct NETCONF port. • Ensure that the device is assigned to a site. To assign the device to a site, in the **Inventory** window, hover your cursor over the **Actions** drop-down list and choose **Provision** > **Assign to Site**. • If the device is assigned to a site, update the telemetry settings with the **Force Configuration Push** option under **Actions** > **Telemetry** > **Update Telemetry Settings**.
After upgrading, the smart account is missing.	Restart the license management service followed by the license manager tool. If the smart account details are not reflected after the restart, add the smart account details manually. If the smart account addition fails, contact customer support for further assistance.

Issue	Possible Cause and Solution
The license usage or purchase count doesn't match in the **License Manager Overview** window.	For switches: • If there is a mismatch in the license count, do the following: • For non-SLP devices (Cisco IOS XE Release 17.3.1 and earlier), resync the devices. • For SLP devices (Cisco IOS XE Release 17.3.2 and later), follow the reporting workflow. • In the case of stacked switches, each stack uses one license. So, the license usage count is based on the number of stacks and not the number of switches. • For the purchase count mismatch, use the **Refresh** option in the **License Manager Overview** window to resync the Cisco Smart Software Manager (CSSM). For routers: • If there is a mismatch in the license count, do the following: • For non-SLP devices (Cisco IOS XE Release 17.3.1 and earlier), resync the devices. • For SLP devices (Cisco IOS XE Release 17.3.2 and later), follow the reporting workflow. • For the purchase count mismatch, use the **Refresh** option in the **License Manager Overview** window to resync the Cisco Smart Software Manager (CSSM). For wireless controllers: • If there is a mismatch in the license count, do the following: • For non-SLP devices (Cisco IOS XE Release 17.3.1 and earlier), resync the devices. • For SLP devices (Cisco IOS XE Release 17.3.2 and later), follow the reporting workflow. • In the case of wireless controllers, licenses are used by the connected APs only. If the wireless controller has no associated APs, licenses are not used. • For the purchase count mismatch, use the **Refresh** option in the **License Manager Overview** window to resync the CSSM. • The license count is not updated every time an AP connects or disconnects from a wireless controller. It takes up to eight hours for the license to be used.

Issue	Possible Cause and Solution
Smart account addition issues.	Perform the following checks: • Use the following commands to check the CSSM reachability: • **openssl s_client -connect tools.cisco.com:443** • **openssl s_client -connect swapi.cisco.com:443** If a proxy server is configured, check if the above URLs are reachable through the proxy server. • Ensure that the network firewall or the proxy server is configured to allow the IP traffic between the appliance and the CSSM to use the Smart Account feature.

RMA Service Troubleshooting

The Return Material Authorization (RMA) workflow in Catalyst Center lets you replace failed devices quickly. The following sections provide troubleshooting information for some common issues in the RMA workflow.

Mark a Device for Replacement

The following table provides troubleshooting information for issues that might occur while marking a device for replacement.

Issue	Possible Cause and Solution
The software image wasn't imported in the image repository.	Import the software image of the faulty device from the **Design** > **Image repository** window.
Network readiness failed.	• This issue can happen with fabric devices, where there's no valid neighbor device to create a temporary DHCP server. You can onboard the replacement device through inventory and use the **Replace Device** workflow to replace the device. • Marking a device for replacement is not allowed if there's an ongoing LAN automation session. • Plug and Play (PnP) onboarding is not supported for Class A and Class B network types. You can onboard the device through inventory and use the **Replace Device** workflow to replace the device.

The Replace Device Workflow

The following table provides troubleshooting information for any issues that might occur in the replace device workflow steps.

Workflow Step	Troubleshooting Steps
Claim the replacement device.	Check the device credentials in **Network Settings**. Claiming fails if the credentials are incorrect.

Workflow Step	**Troubleshooting Steps**
Run the readiness checks for device replacement.	Check the SCP or HTTP reachability of the device.
Distribute and activate the software image to the replacement device.	Check the image versions and modes of the faulty and new devices. If the version and mode are the same, skip the SWIM step to avoid the image activation. Expand the status message in the step for more information on the issue.
Deploy licenses to the replacement device.	Catalyst Center does not support legacy licenses. Deploy the legacy license manually and retry the workflow.
Provision VLAN configurations.	Check the SCP or HTTP reachability of the device. For HTTPS, check if the device has the Catalyst Center CA certificate.
Provision startup configurations.	Check the SCP or HTTP reachability of the device. For HTTPS, check if the device has the Catalyst Center CA certificate.
Check for reachability of the replacement device.	A faulty device should have a static IP address except for extended nodes. Check the SNMPv2, CLI, and NETCONF reachability of the device from Catalyst Center.
Deploy SNMPv3 credentials to the replacement device.	Check the SNMPv2 reachability of the device for any reachability issues.
Synchronize the replacement device.	Check the Catalyst Center device inventory for more details.
Create the PKI certificate.	Check the Catalyst Center provisioning summary for more details on the issue.
Update Cisco ISE.	Check the device in Cisco ISE and Catalyst Center. Check the serial numbers, hostnames, and IP addresses of both faulty and replacement devices in Cisco ISE. The faulty device in Cisco ISE should be updated with the new serial number.

Post RMA Workflow Changes

The following table provides troubleshooting information for issues that might occur after completing the RMA workflow.

Issue	**Possible Cause and Solution**
In replacement devices, configurations are missing.	Check the **Config Drift** tab under device details for configuration change history. Less than two entries in the history indicates an issue in archiving configuration changes. For further assistance, contact customer support.

Grouping Service Troubleshooting

The following table provides troubleshooting information for some common issues in the grouping service.

Issue	Possible Cause and Solution
How to check if the grouping service is working?	• From the top-left corner, click the menu icon and choose **Design** > **Network Hierarchy** and check if the site hierarchy is displayed. • Go to **Provision** > **Inventory** and click **Tag** to check if the tags are displayed in the device inventory list.
How to enable debug logs for the grouping service?	In the Catalyst Center homepage, go to **System** > **Settings** > **Debugging Logs** and enable the debugging logs for **grouping-service**.

SWIM Services Troubleshooting

The following table provides troubleshooting information for some common issues in SWIM services.

Issue	Possible Cause and Solution
The software image is marked golden but the device doesn't show **Needs Update** in the **Software Image** column.	Perform the following checks: • Ensure that the golden marking is done at the same site where the device is present or at the global level. • Ensure that the device family is mapped correctly. For example, if the device is supervisor, the respective supervisor family should be used for golden marking. • If the device is Cisco Catalyst 9407R Supervisor Engine-1, the golden marking should be done at the supervisor family and not at the Cisco Catalyst 9407R switch. • Only in the case of PnP flow, golden marking or golden image updating must be done on the same device family which was used while assigning the image. For example, consider that during PnP, the Cisco Catalyst 9407R Switch is used for assigning the image. After the device has been claimed and the golden image is updated, you need to assign the image at Cisco Catalyst 9407R Supervisor Engine-1 level. For any new device claim with the latest image, the golden marking is done at the Cisco Catalyst 9407R Switch. • Check if any native site-level golden marking is overriding the global-level golden marking or if any golden marking is done through device tagging.

Issue	**Possible Cause and Solution**
Cisco.com connectivity issues.	• For firewall issues, access the following URLs to check the SSL/TLS certificate revocation status using OCSP/CRL. Access must be allowed either directly or through the proxy server. • http://ocsp.quovadisglobal.com • http://crl.quovadisglobal.com/* • http://*.identrust.com • If the latest software image or the suggested image is not listed for each device family, ensure that Cisco.com account credentials are provided in the settings or the **Image Repository** window and the accounts have the permission to download the software images.
SWIM upgrade flow issues.	For distribution issues, do the following: • Ensure that the precheck runs are successful and check whether the **File transfer check** is a success or warning. • If an HTTPS copy fails, push the Catalyst Center root certificate and then retry the copy operation. If the HTTPS copy retry fails, check the certificate validity and ensure that the device is reachable from Catalyst Center. Check the device reachability using the IP ping test for SCP failures also. If the issue persists, contact customer support. For activation issues, do the following: During activate or commit operation, if there is any time-out error, check whether the device is upgraded to the golden image. You can verify this from the Catalyst Center **Inventory** window by changing the **Focus** drop-down list to **Software Images**, where the software image version shows the currently running image version. You can also connect to the device using the command runner to check if the device is running the same image version as that of the golden image.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.