Troubleshoot No Assurance Data from WLC 9800 in Catalyst Center

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Troubleshoot No Assurance Data from WLC in Catalyst Center

- Use the Assurance "Troubleshoot" Machine Reasoning Engine (MRE) Tool in WLC360
- Conclusion: Device Connectivity
  - Data and verification of assessment
  - Items to troubleshoot and check
  - IP Connectivity
- Conclusion: Device "not currently managed by Catalyst Center"
- Conclusion: "DNAC-CA (swim) certificate" issues
- Conclusion: "Serial Number of the sdn-network-infra-iwan certificate" issue

Inbound Data Verification

Perform 'Forced' Telemetry Update

Introduction

This document describes how to troubleshoot when Catalyst Center does not show any Assurance data for a Catalyst 9800 Series WLC.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Use of the Catalyst Center maglev CLI
- Basic Linux foundation
- Knowledge of certificates on Catalyst Center and on the Catalyst 9800 platform

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst Center appliance 2nd and 3rd generations, version 2.3.7.7 and later
- Catalyst 9800 Series Wireless LAN Controller (WLC)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure

that you understand the potential impact of any command.

Note: While this document was written based on 2.3.7.9. This function is also present in 3.1.X releases.

Note: The Catalyst 9800 WLC must be already discovered by Catalyst Center and assigned to a site, and must run a compatible Cisco IOS® XE version. For more details about interoperability, refer to the Catalyst Center Compatibility Matrix.

Background Information

At the moment of site assignment, the Catalyst Center will push Telemetry configuration to the 9800 on top of the SNMP and Syslog configurations.

Note: This example is from a Catalyst 9800-CL Cloud Wireless LAN Controller. Some details can differ when you use a physical Catalyst 9800 Series appliance; X.X.X.X is the Virtual IP (VIP) address of the Catalyst Center enterprise interface and Y.Y.Y.Y is the management IP address of the WLC.

<#root>

```
crypto pki trustpoint sdn-network-infra-iwan
 enrollment pkcs12
 revocation-check crl
 rsakeypair sdn-network-infra-iwan

crypto pki trustpoint DNAC-CA
 enrollment mode ra
 enrollment terminal
 usage ssl-client
 revocation-check crl none
 source interface GigabitEthernet1

crypto pki certificate chain sdn-network-infra-iwan
 certificate 14CFB79EFB61506E
  3082037D 30820265 A0030201 02020814 CFB79EFB 61506E30 0D06092A 864886F7
  <snip>
        quit

 certificate ca 7C773F9320DC6166
  30820323 3082020B A0030201 0202087C 773F9320 DC616630 0D06092A 864886F7
  <snip>
        quit

crypto pki certificate chain DNAC-CA
 certificate ca 113070AFD2D12EA443A8858FF1272F2A
  30820396 3082027E A0030201 02021011 3070AFD2 D12EA443 A8858FF1 272F2A30
  <snip>
        quit

telemetry ietf subscription 1011
 encoding encode-tdl
 filter tdl-uri /services;serviceName=ewlc/wlan_config
```

```
 source-address
```

Y.Y.Y.Y

```
 stream native
 update-policy on-change
 receiver ip address
```

X.X.X.X

```
 25103 protocol tls-native profile sdn-network-infra-iwan

telemetry ietf subscription 1012
<snip - many different "telemetry ietf subscription" sections - which ones depends on
Cisco IOS® version and Catalyst Center version>

network-assurance enable
network-assurance icap server port 32626
network-assurance url https://
```

X.X.X.X

```
network-assurance na-certificate PROTOCOL_HTTP
```

X.X.X.X

```
 /ca/ pem
```

Troubleshoot No Assurance Data from WLC in Catalyst Center

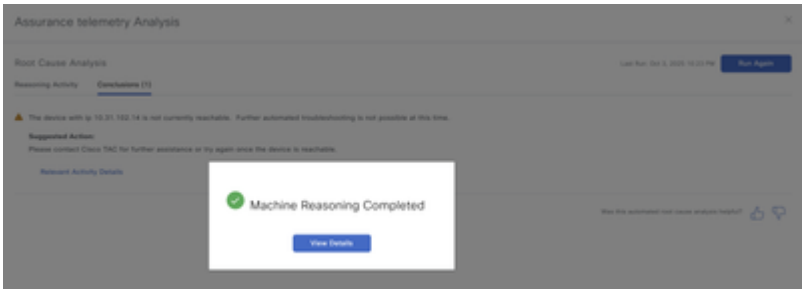
Use the Assurance "Troubleshoot" Machine Reasoning Engine (MRE) Tool in WLC360

Go to the **WLC360** page. Next to the health, the user will see blue text "**Troubleshoot**".



Click on it and run the Machine Reasoning Engine.

Allow the reasoning engine to run to completion.



Check the "**Conclusions**" tab to see what the possible issues are. If one receives a complete with no issues in

the "Conclusion", then please skip to the Inbound Data Verification section of this document.

If you do not see this "**Troubleshoot**" link, then you can manually run this on the **Tools > Network Reasoner** page in the GUI. Find the "**Assurance Telemetry Analysis**" workflow.



Conclusion: Device Connectivity

Data and verification of assessment

First, go to the Inventory page and ensure the WLC in question is managed using the WLC's Wireless Management IP address.

For 9800 appliances: *show wireless interface summary*



For 9800-CL: *show ip interfaces brief | i GigabitEthernet2*
Note: This is assumes the user followed the Deployment Guide at https://www.cisco.com/c/en/us/td/docs/wireless/controller/9800/technical-reference/c9800-cl-dg.html#Introduction



Now, go to the Catalyst Center's **Inventory** page.



This verifies there are connectivity issues between the Catalyst Center and this device.

Items to troubleshoot and check

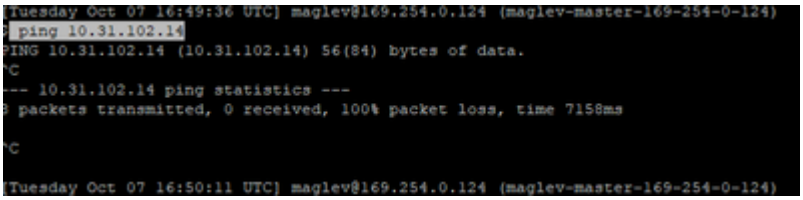
IP Connectivity

From the Main Menu go to the **System > Settings** page. Then, on the left banner go to the "**Trust & Privacy**" section and select "**IP Access Control**." An alternative method is to use the global search and

search for "*IP Access Control*"



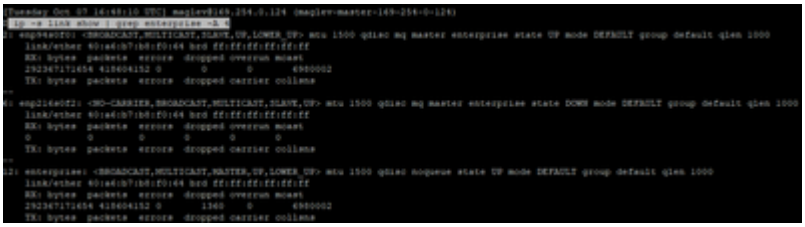
Please make sure the settings here allow connectivity to the device in question. Next, verify one can reach the end device via ICMP. To do this log into the CLI of Catalyst Center and issue the command "*ping [IP_Address]*" as seen in this output.



The next item to look into is the output of the "*traceroute*" command from the Catalyst Center CLI.



Next, verify there are no link issues on the Catalyst Center using the command "*ip -s link show | grep enterprise -A 4*"



If the interface metrics look acceptable, then the next step is to perform a packet capture (PCAP) from both sides of the connection. This guide recommends performing the first set of PCAPs on the devices in question. In this example, the two devices here are a 9800 and the Catalyst Center with the VIP. If that is not possible, then please run the PCAPs as close to the devices as possible.

If packets are being sent into the network but not making it through the wired infrastructure, then please investigate the wired network for things such as asynchronous routing, firewalls, NATs, and ACLs blocking the packets. Once these are resolved, please re-run the Assurance "**Troubleshoot**" MRE.

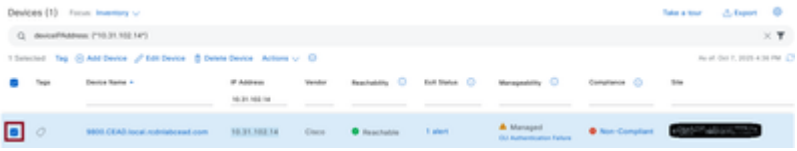
Conclusion: Device "not currently managed by Catalyst Center"



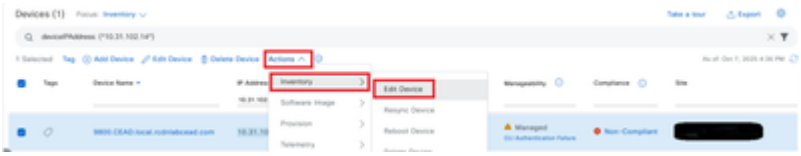
As of today 2.3.7.10, the workflow output can state to contact the TAC. There are actions that can be performed before reaching out to the TAC or determining if a TAC case is the correct immediate course of action. First go to the Inventory page and find the device in question; **Main Menu > Provision > Inventory**. Here is an example of what an incorrectly configured SSH password looks like



Now the next item to check is that the "Reachability" status does not show "Unreachable". If it shows "Unreachable" or "Unknown", then please go to the "Device Connectivity or Credential Failure" section of this guide before engaging the TAC. If it shows "Ping Reachable" or "Reachable," then one can move on to troubleshooting the credentials used by the Catalyst Center. To do that click the box on the left of the device you wish to investigate as shown. The box will turn blue with a blue check mark.

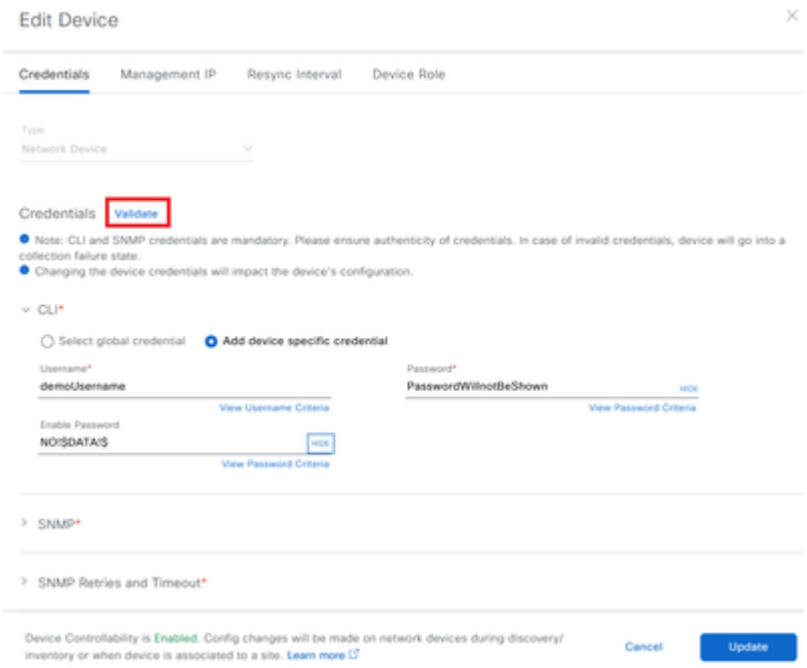


Then click on "**Actions**", "**Inventory**", and finally "**Edit Device**" as shown:

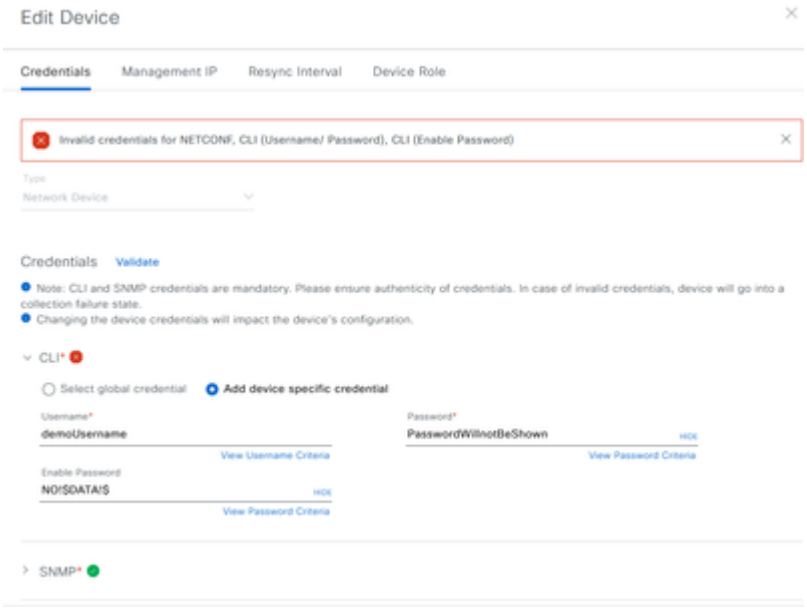


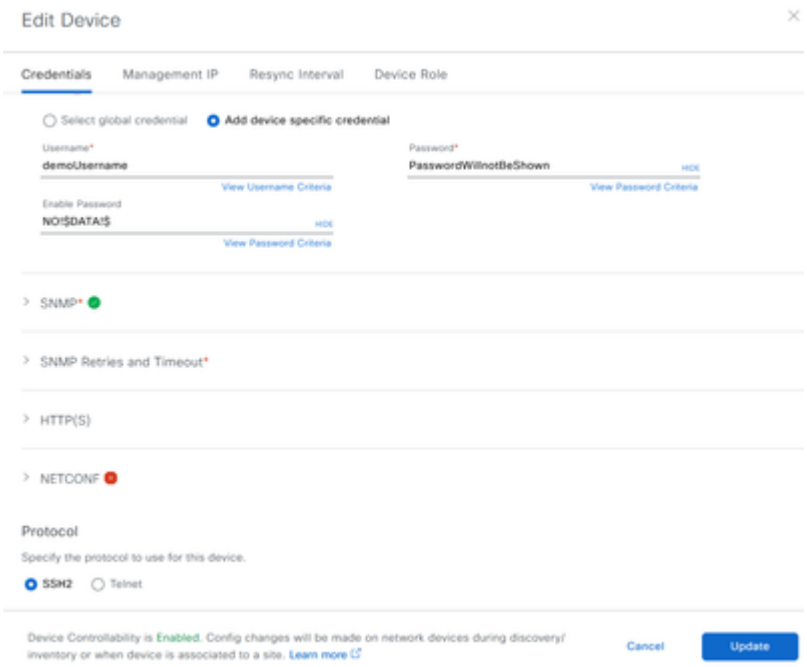
This action will bring up a new window that will allow you to "**Validate**" this configuration. Please see this screenshot for an example.

Note: On this page the "Username" will be shown in clear text, but the "Passwords" will not. Instead the Catalyst Center will show the passwords as "NO!$DATA!$".



This is an example of what correct credentials look like. See the SNMP and invalid credentials, see CLI and Netconf.





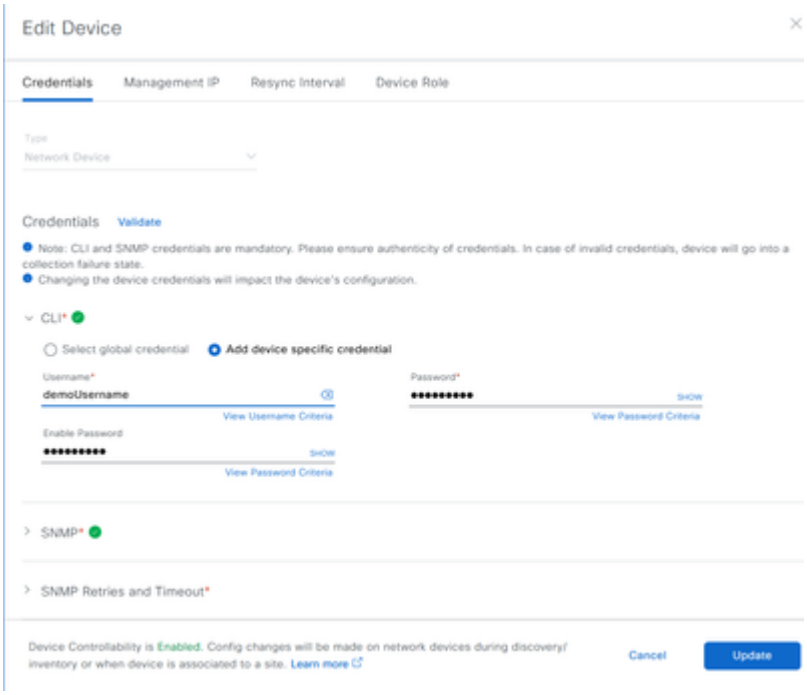
Note: Wireless access points (APs) will not be managed this way. All AP data will be through the WLC.

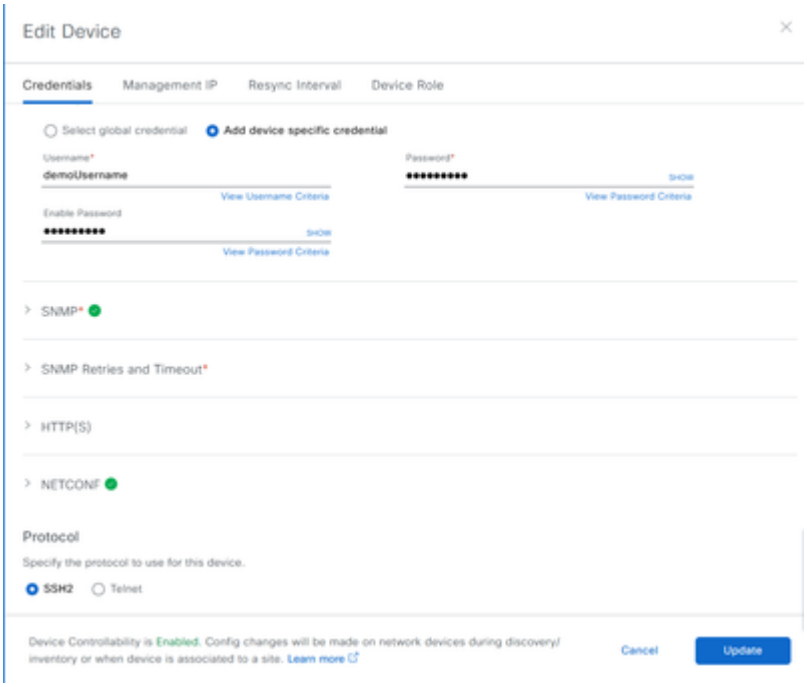
CLI (SSH) access is mandatory for all devices.

SNMP with a minimum of read only access is mandatory for all devices.

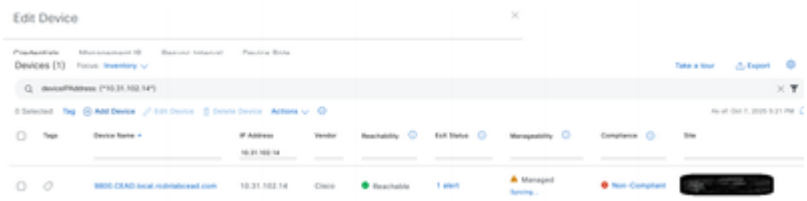
Netconf is mandatory for 9800 (Cisco IOS® XE based) WLCs. Netconf will provide additional monitoring such as PoE Dashboards for Cisco IOS® XE based switches and therefore is optional. Netconf is not used by AireOS or Cisco IOS® based devices.

After correcting all the issues and running the "**Validate**" option again, one can see this:





After the errors have been addressed, then click on the "**Update**" button in the lower left. When this is done, the Catalyst Center will queue this device up for a "Sync". If the queue is empty, then the "Sync" will start immediately as shown.



After this is done, then please go back to the "**Troubleshoot**" MRE output to see if other items need to be addressed. If nothing else comes up, please wait for 15-20 minutes to see updated information. Please reach out to the TAC for further assistance if the information does not update after that time.

Conclusion: "DNAC-CA (swim) certificate" issues

Here we have a few possibilities:

- The certificate is for a different Catalyst Center
- The "current date/time" on the device is outside the valid range
- The certificate has been replaced, and the device is using the older certificate.

Please see which one the MRE is indicating. From here, we can then go to the 9800 and run a few commands to see which issue is causing the problem. First to determine the time and date the device is using run the *show clock* command.

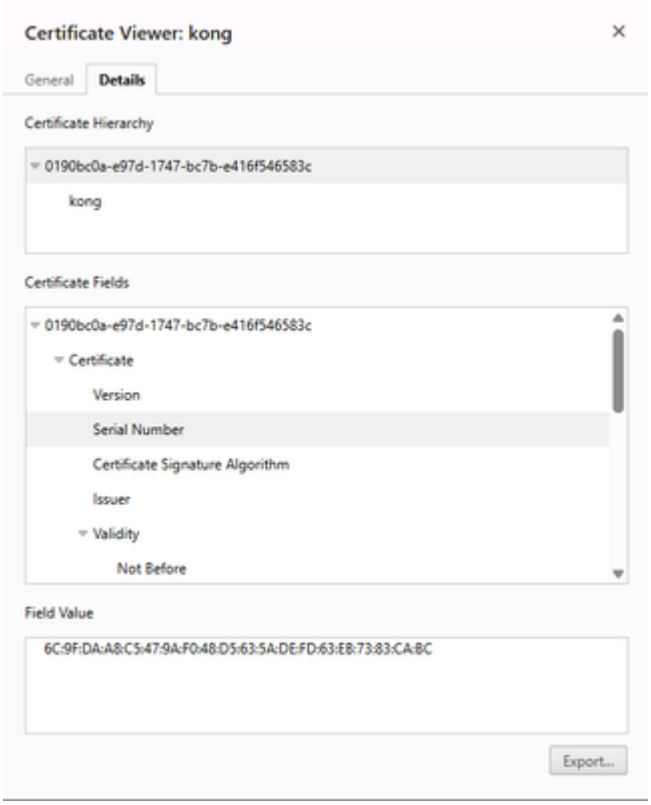
```
9800.CEAD.local#show clock
*02:30:48.038 UTC Thu Oct 9 2025
9800.CEAD.local#
```

Then, run *show crypto pki certificates DNAC-CA* to pull up details of the DNAC-CA certificate.

```
9800.CEAD.local#show crypto pki certificates DNAC-CA
CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C9FDAA8C5479AF048D5635ADEFD63EB7383CABC
  Certificate Usage: General Purpose
  Issuer:
    ou=Cisco DNA Center
    o=Cisco Systems
    cn=0190bc0a-e97d-1747-bc7b-e416f546583c
  Subject:
    ou=Cisco DNA Center
    o=Cisco Systems
    cn=0190bc0a-e97d-1747-bc7b-e416f546583c
  Validity Date:
    start date: 20:45:15 UTC Feb 2 2024
    end   date: 20:45:15 UTC Oct 29 2026
  Associated Trustpoints: DNAC-CA
  Storage: nvram:CiscoDNACent#CABCCA.cer


9800.CEAD.local#
```

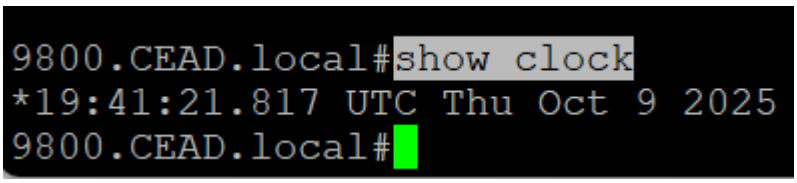
First, compare the "start date" and "end date" with the current date and time the device believes it is. If the **Conclusion** states the certificate does not match, then on the browser pull up the certificate information. The serial number must match. This is an example from Chrome of a matching certificate serial number.



Conclusion: "Serial Number of the sdn-network-infra-iwan certificate" issue



First, verify the date on the device is correct



Then, pull up the sdn-network-infra-iwan certificate details with *show crypto pki certificates sdn-network-infra-iwan*

```
9800.CEAD.local#show crypto pki certificates sdn-network-infra-iwan
Certificate
  Status: Available
  Certificate Serial Number (hex): 676164CD0EED70C9
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: 9800.CEAD.local.rcdnlabcead.com
    cn=C9800-L-C-K9 [redacted] sdn-network-infra-iwan
    hostname=9800.CEAD.local.rcdnlabcead.com
  Validity Date:
    start date: 02:26:47 UTC Oct 4 2025
    end   date: 02:26:47 UTC Oct 4 2026
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#70C9.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C45E5EC0CB658E1
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 23:21:50 UTC Feb 2 2024
    end   date: 23:21:50 UTC Feb 2 2039
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#58E1CA.cer
```

In that please verify that the validity dates are within the dates the device believes it is.

```
9800.CEAD.local#show crypto pki certificates sdn-network-infra-iwan
Certificate
  Status: Available
  Certificate Serial Number (hex): 676164CD0EED70C9
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: 9800.CEAD.local.rcdnlabcead.com
    cn=C9800-L-C-K9_[redacted]_sdn-network-infra-iwan
    hostname=9800.CEAD.local.rcdnlabcead.com
  Validity Date:
    start date: 02:26:47 UTC Oct 4 2025
    end   date: 02:26:47 UTC Oct 4 2026
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#70C9.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C45E5EC0CB658E1
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 23:21:50 UTC Feb 2 2024
    end   date: 23:21:50 UTC Feb 2 2039
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#58E1CA.cer
```

Next go to the Catalyst Center and verify the certificate serial number matches.

```
9800.CEAD.local#show crypto pki certificates sdn-network-infra-iwan
Certificate
  Status: Available
  Certificate Serial Number (hex): 676164CD0EED70C9
  Certificate Usage: General Purpose
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    Name: 9800.CEAD.local.rcdnlabcead.com
    cn=C9800-L-C-K9_[redacted] _sdn-network-infra-iwan
    hostname=9800.CEAD.local.rcdnlabcead.com
  Validity Date:
    start date: 02:26:47 UTC Oct 4 2025
    end   date: 02:26:47 UTC Oct 4 2026
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#70C9.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 6C45E5EC0CB658E1
  Certificate Usage: Signature
  Issuer:
    cn=sdn-network-infra-ca
  Subject:
    cn=sdn-network-infra-ca
  Validity Date:
    start date: 23:21:50 UTC Feb 2 2024
    end   date: 23:21:50 UTC Feb 2 2039
  Associated Trustpoints: sdn-network-infra-iwan
  Storage: nvram:sdn-network-#58E1CA.cer
```

Go to the **Main Menu > System > Settings** page. On that page find the "**Device Certificate**" page. On that page, filter down to the device in question and check that the "**Certificate Serial Number**" matches.

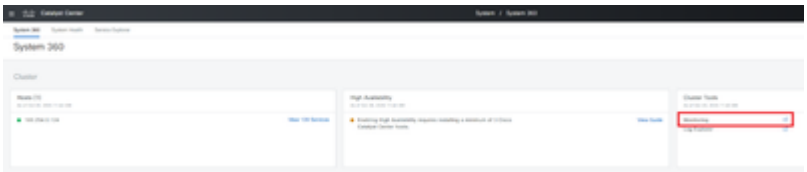


If this does not match, please verify that the device is expected to be here and not managed by another Catalyst Center cluster. If the failure is recent or the certificate is yet to expire, please contact the TAC for further root cause analysis if desired. Otherwise go to the "**Inventory**" page and ensure the device is "Reachable" and "Managed" with green check marks. If there is an issue on this page, then please go to section Conclusion: Device "not currently managed by Catalyst Center" of this guide and complete the instructions.

If everything is all green and fully managed, then please perform a **Forced Telemetry** update see the section Perform 'Forced' Telemetry Update.

Inbound Data Verification

Navigate to Grafana by going to **System > System 360 > Monitor**. This will bring up a new screen for Grafana



Then, proceed to the **Assurance – Device Processor** dashboard by clicking on the magnifying glass in the left column and typing *Device Processor*



In the table "**Received WLC schema per 5min**" check the "**Memory**" number. This number matches the number of Catalyst 9800 (Cisco IOS® XE) WLCs sending traffic.



Perform ‘Forced’ Telemetry Update

Go to **Inventory** and select **Update Telemetry Settings** as shown.

