Manage Catalyst 9800 Wireless Controller Series with Prime Infrastructure with SNMP V2 and V3 and NetCONF

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Configure

- Ports Used
- SNMPv2 Configuration on Cat 9800 WLC
- SNMPv3 Configuration on Cat 9800 WLC
- Netconf Configuration on the Cat 9800 WLC
- Configure (Prime Infrastructure 3.5 and Later)

Verify

- Verify Telemetry Status

Troubleshoot

- Troubleshooting on Prime Infrastructure
- Troubleshooting on Catalyst 9800 WLC
- Delete All the Telemetry Subscription from the WLC Configuration

Check for Subscription ID for AP Information

Migration from PI to Cisco Catalyst Center

Introduction

This document describes how to integrate Catalyst 9800 Series Wireless Controllers (C9800 WLC) with Prime Infrastructure (3.x).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- C9800 WLC
- Prime Infrastructure (PI) Version 3.5
- Simple Network Management Protocol (SNMP)

Components Used

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

- C9800 WLC
- Cisco IOS XE Gibraltar 16.10.1 to 17.3

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: Prime Infra 3.8 only supports 17.x 9800 WLCs. Clients do not show up on Prime Infrastructure if you try to manage a 16.12 WLC with Prime Infra 3.8.

Configure

In order for Prime Infrastructure to configure, manage and monitor Catalyst 9800 Series Wireless LAN Controllers, it needs to be able to access C9800 via CLI, SNMP, and Netconf. When you add C9800 to Prime Infrastructure, telnet/SSH credentials as well as SNMP community string, version, and so on, need to be specified. PI uses this information to verify reachability and to inventory C9800 WLC. It also uses SNMP to push configuration templates as well as support traps for Access Point (AP) and client events. However, in order for PI to gather AP and Client statistics, Netconf is leveraged. Netconf is not enabled by default on C9800 WLC and needs to be manually configured via CLI on the 16.10.1 release (GUI available in 16.11.1).

Ports Used

Communication between C9800 and Prime Infrastructure uses different ports.

- All configurations and templates available in Prime Infra get pushed via SNMP and CLI. This uses UDP port 161.
- Operational data for C9800 WLC itself is obtained over SNMP. This uses UDP Port 162.
- AP and client operational data leverages streaming telemetry.

Prime Infrastructure to WLC: TCP port 830 - This is used by Prime Infra to push the telemetry configuration to 9800 devices (using Netconf).
WLC to Prime Infrastructure: TCP port 20828 (for Cisco® IOS XE 16.10 and 16.11) or 20830 (for Cisco IOS XE 16.12,17.x and later).

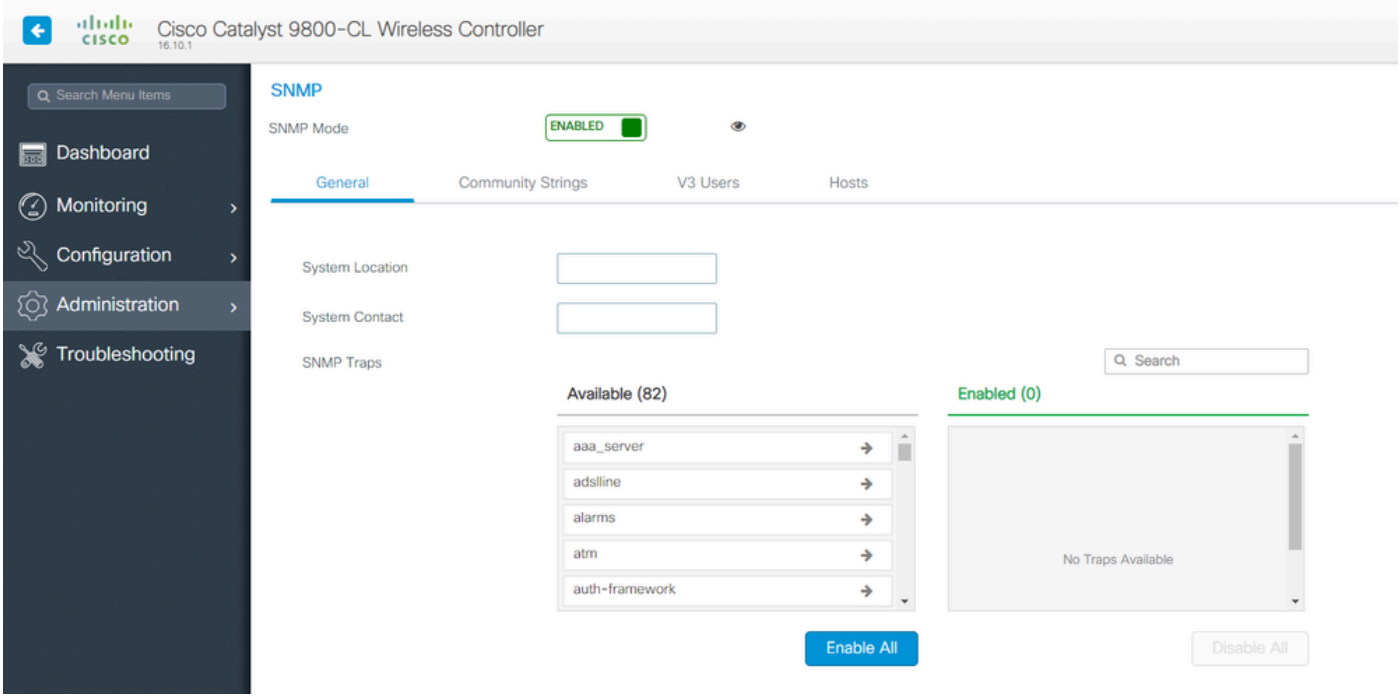
Note: Keepalives are sent every 5 seconds even when there is no telemetry to report.

Note: In case there is a firewall between Prime Infrastructure and C9800, be sure to open these ports to establish communication.

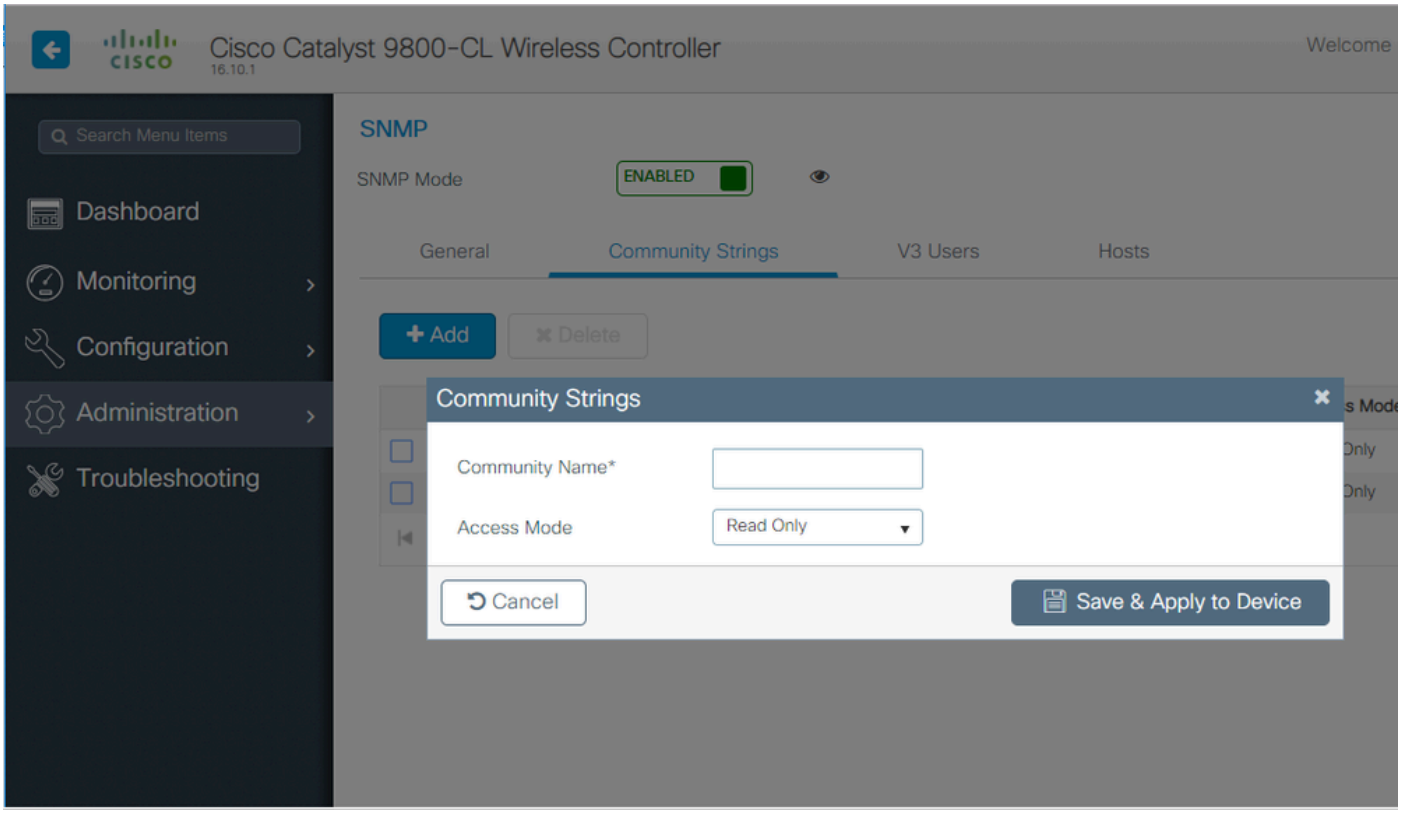
SNMPv2 Configuration on Cat 9800 WLC

GUI:

Step 1. Navigate to **Administration > SNMP > Slide to Enable SNMP.**



Step 2. Click on **Community Strings** and create a Read-Only and a Read-Write community name.



CLI:

```
(config)#snmp-server community <snmpv2-community-name>
(optional)(config)# snmp-server location <site-location>
(optional)(config)# snmp-server contact <contact-number>
```

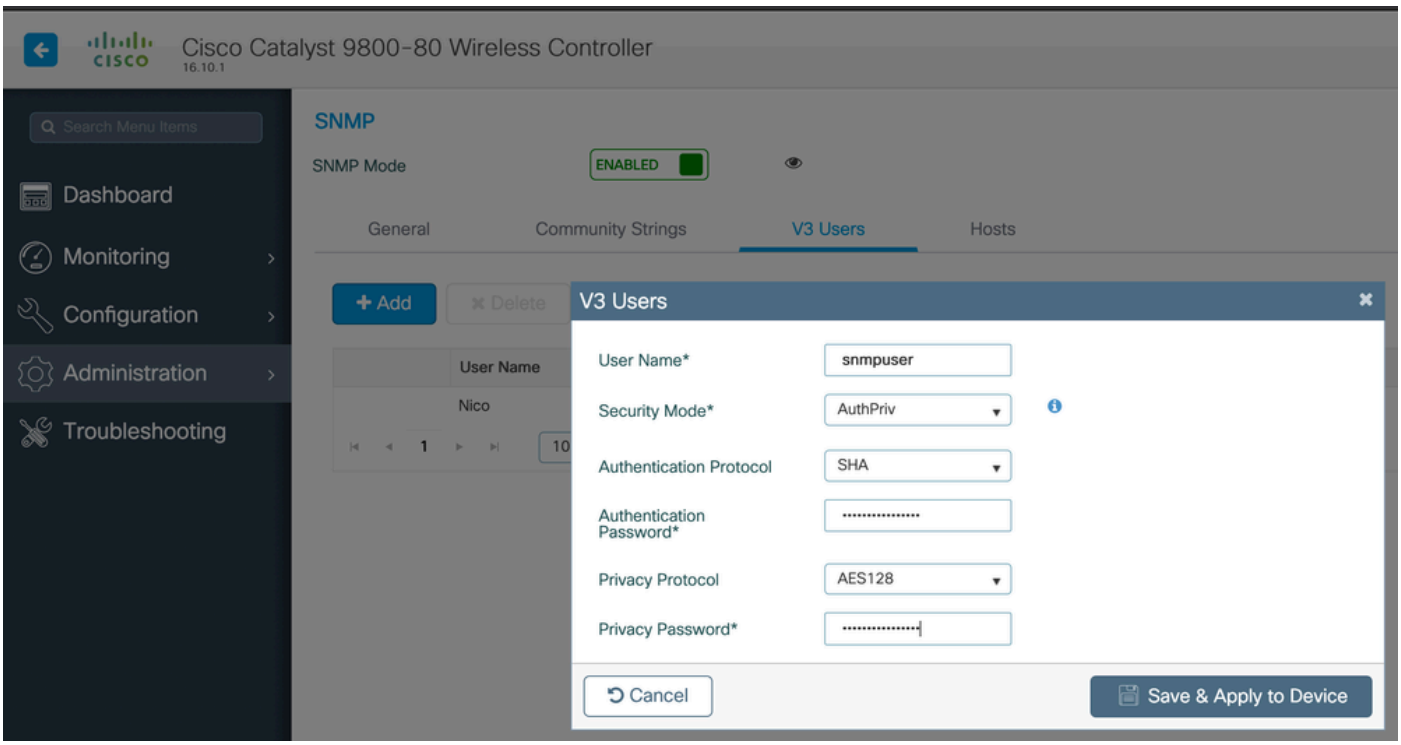
SNMPv3 Configuration on Cat 9800 WLC

GUI:

> **Note**: As of 17.1 Cisco IOS XE, the web UI only allows you to create read-only v3 users. You need to run the CLI procedure to create a read-write v3 user.

CLI:

Click on **V3 users**and create a user. Choose **authPriv, SHA** and **AES protocols,** and choose long passwords. **MD5** and **DES/3DES** are insecure protocols and although they are still an option in the 9800, they must not be selected and are not fully tested anymore.



> **Note**: SNMPv3 User Config is not reflected on running-configuration. Only SNMPv3 group configuration is seen.

CLI:

```
(config)#snmp-server view primeview iso included
(config)#snmp-server group <v3-group-name> v3 auth write primeview
(config)#snmp-server user <v3username> <v3-group-name> v3 auth {md5 | sha} <AUTHPASSWORD> priv {3des |
```

```
9800#show snmp user

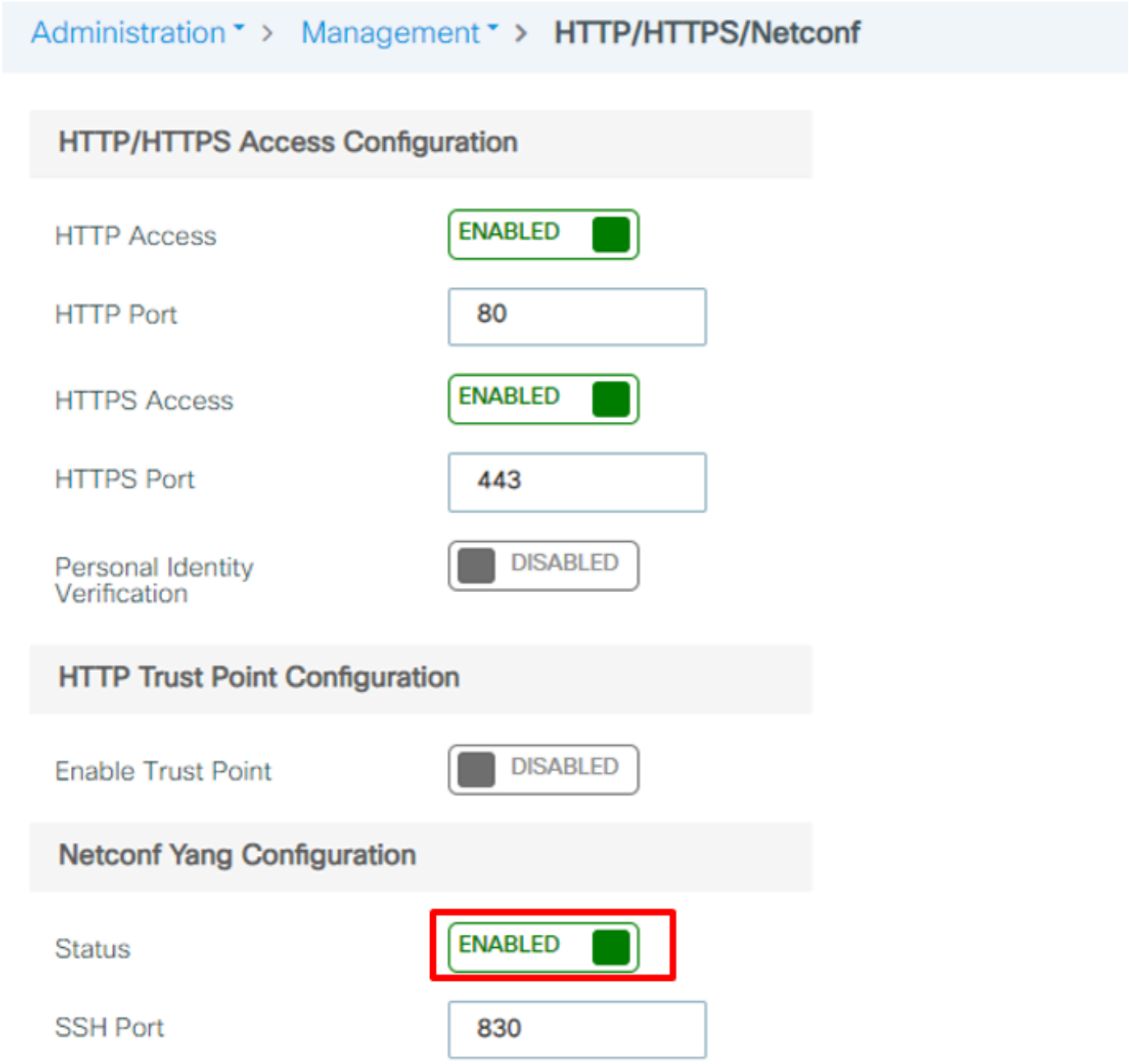
User name: Nico
Engine ID: 800000090300706D1535998C
```

```
storage-type: nonvolatile     active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: SnmpAuthPrivGroup
```

Netconf Configuration on the Cat 9800 WLC

GUI (starting 16.11):

Navigate to **Administration > HTTP/HTTPS/Netconf.**

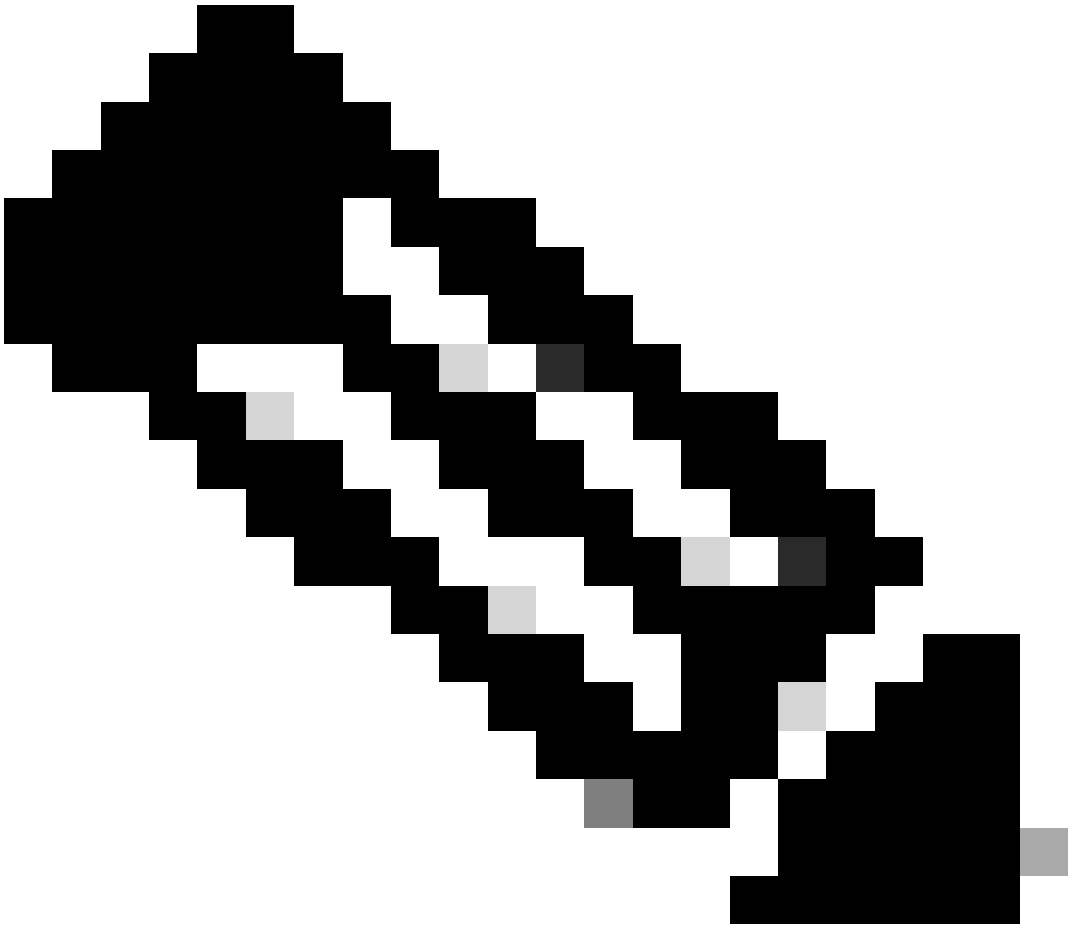


CLI:

```
(config)#netconf-yang
```

Caution: If aaa new-model is enabled on C9800, then you also need to configure:
(config)#aaa authorization exec default <local or radius/tacacs group>
(config)#aaa authentication login default <local or radius/tacacs group>
Netconf on C9800 uses the default method (and you cannot change this) for both aaa authentication login as well as aaa authorization exec. In case you want to define a different method for SSH connections, you can do so under the **line vty** command line. Netconf keeps using the default methods.

Caution: Prime infrastructure, when adding a 9800 controller to its inventory, overwrites the aaa authentication login default and aaa authorization exec default methods you had configured and point them to local authentication only in case Netconf is not already enabled on the WLC. If Prime Infrastructure is able to log in with the Netconf, it does not change the configuration. This means, if you were using TACACS, you lose CLI access after adding the 9800 to Prime. You can revert back those configuration commands afterward and make them point to TACACS if that is your preference.



Note: Only the RSA keys are currently supported on the trustpoint used by NETCONF. EC

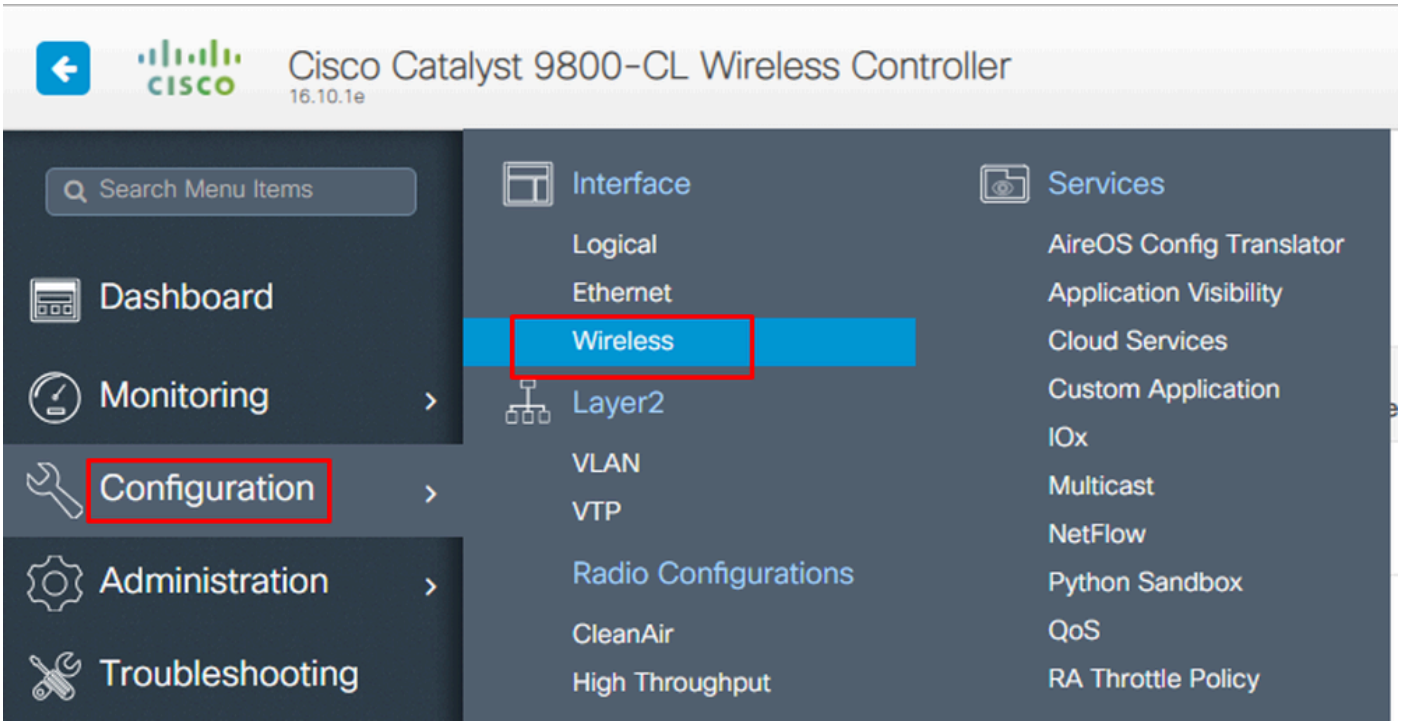
(Elliptic Curve) keys are not yet supported and they cause the ncsshd process to crash if used. You can verify the key being used by the ncsshd process executing the command "show logging process ncsshd internal start last 1 hours | sec key name". A enhancement request is open to add the support for EC keys in future releases :Cisco Bug ID CSCwk02600

Configure (Prime Infrastructure 3.5 and Later)

Step 1. Capture the Wireless Management IP address configured on the Catalyst 9800 WLC.

GUI:

Navigate to **Configuration > Interface: Wireless.**



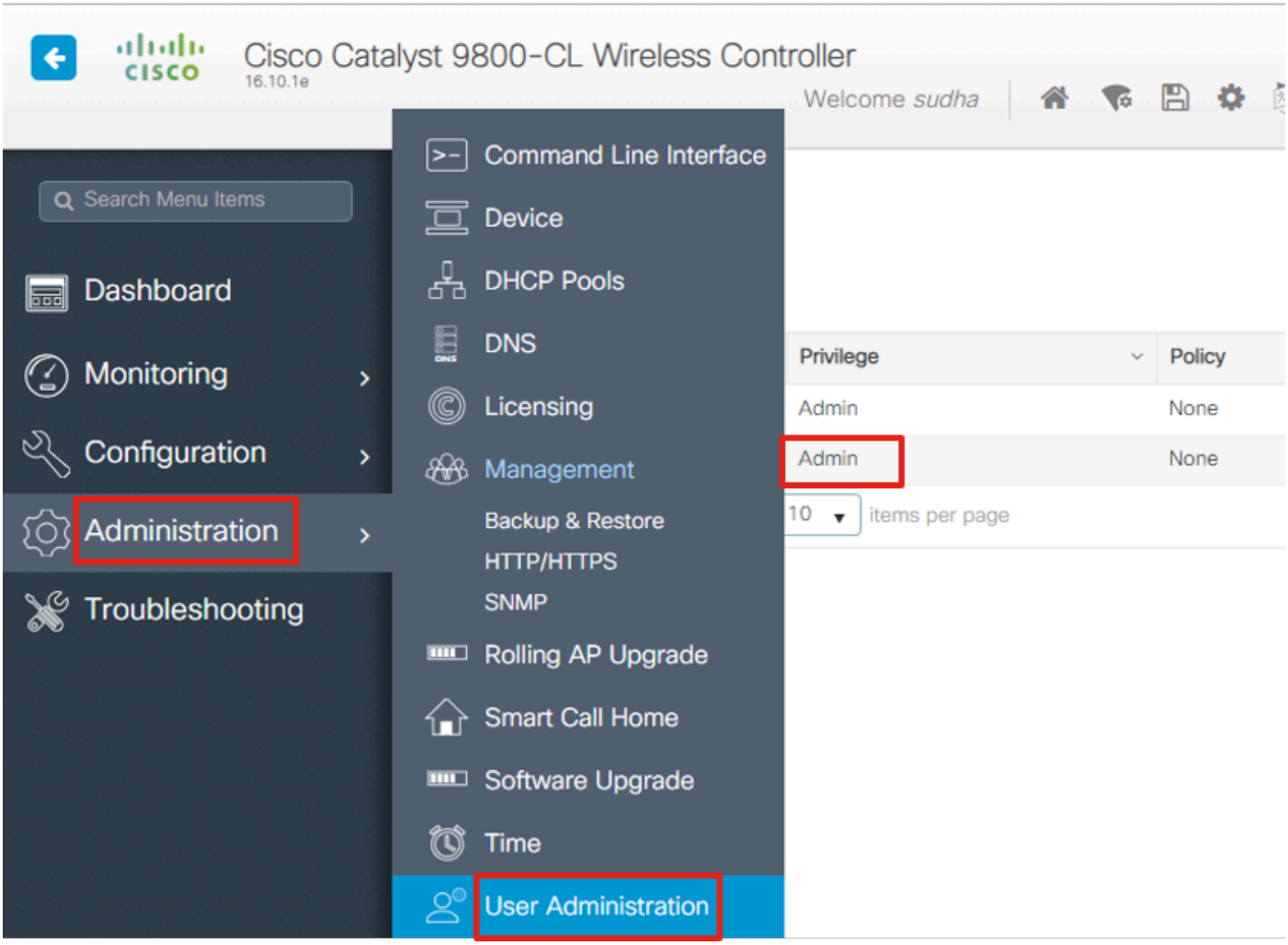
CLI:

```
# show wireless interface summary
```

Step 2. Capture the privilege 15 user credentials as well as enable the password.

GUI:

Navigate to **Administration > User Administration.**



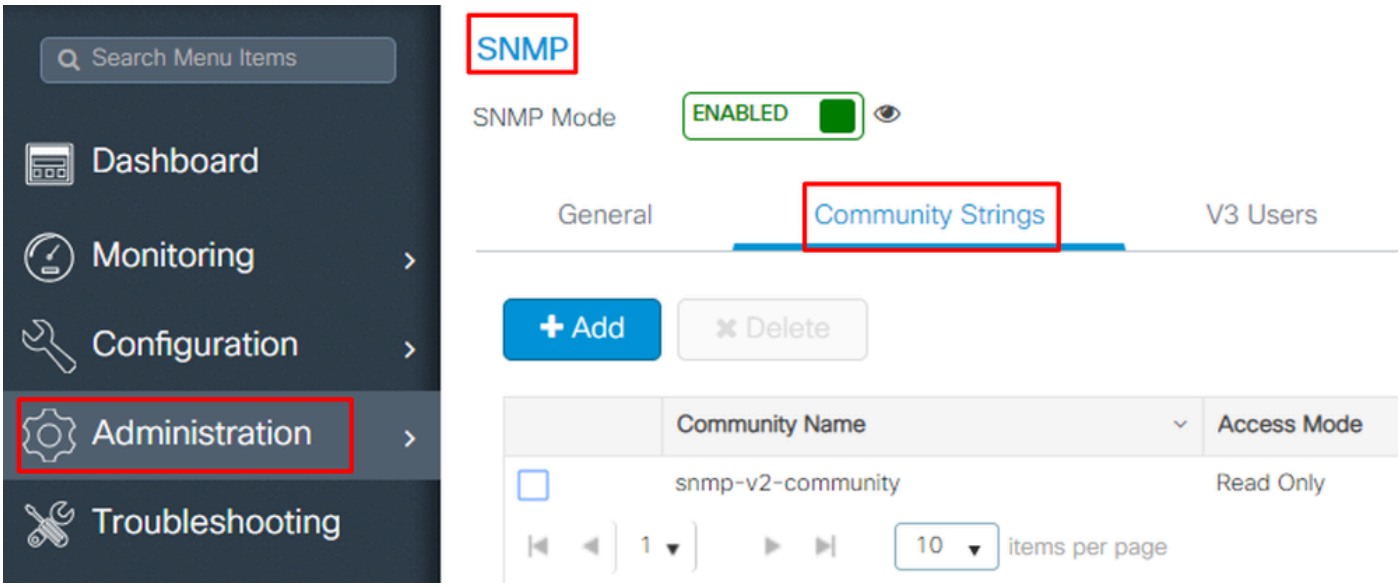
CLI:

```
# show run | inc username
# show run | inc enable
```

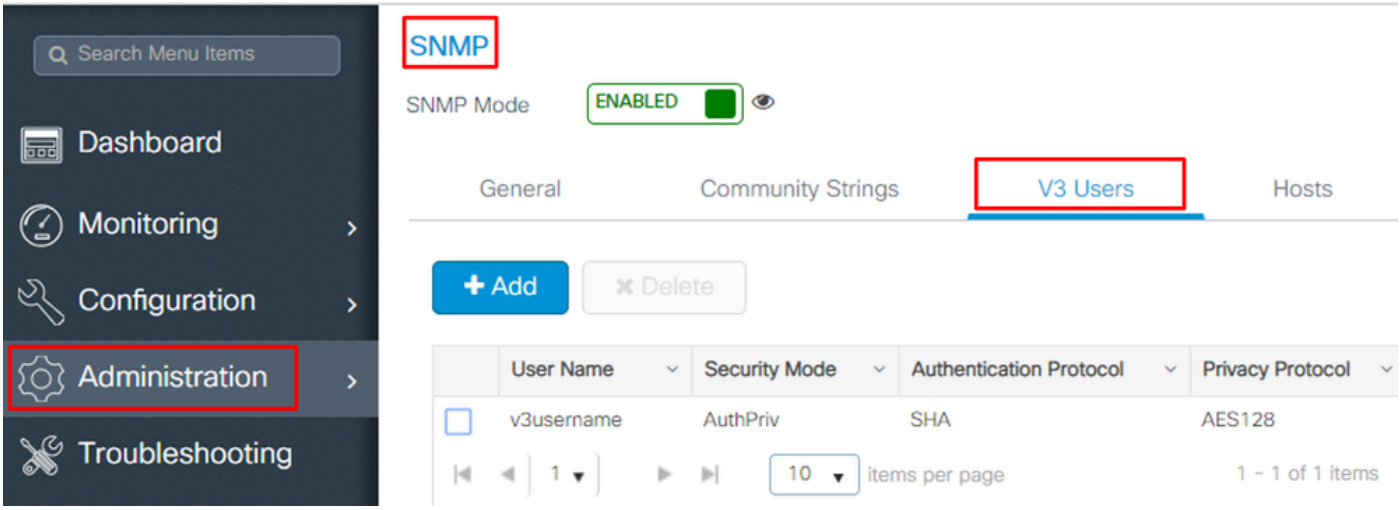
Step 3. Get the SNMPv2 community strings and/or SNMPv3 user as applicable.

GUI:

For SNMPv2, navigate to **Administration > SNMP > Community Strings.**



For SNMPv3, navigate to **Administration > SNMP > V3 Users.**

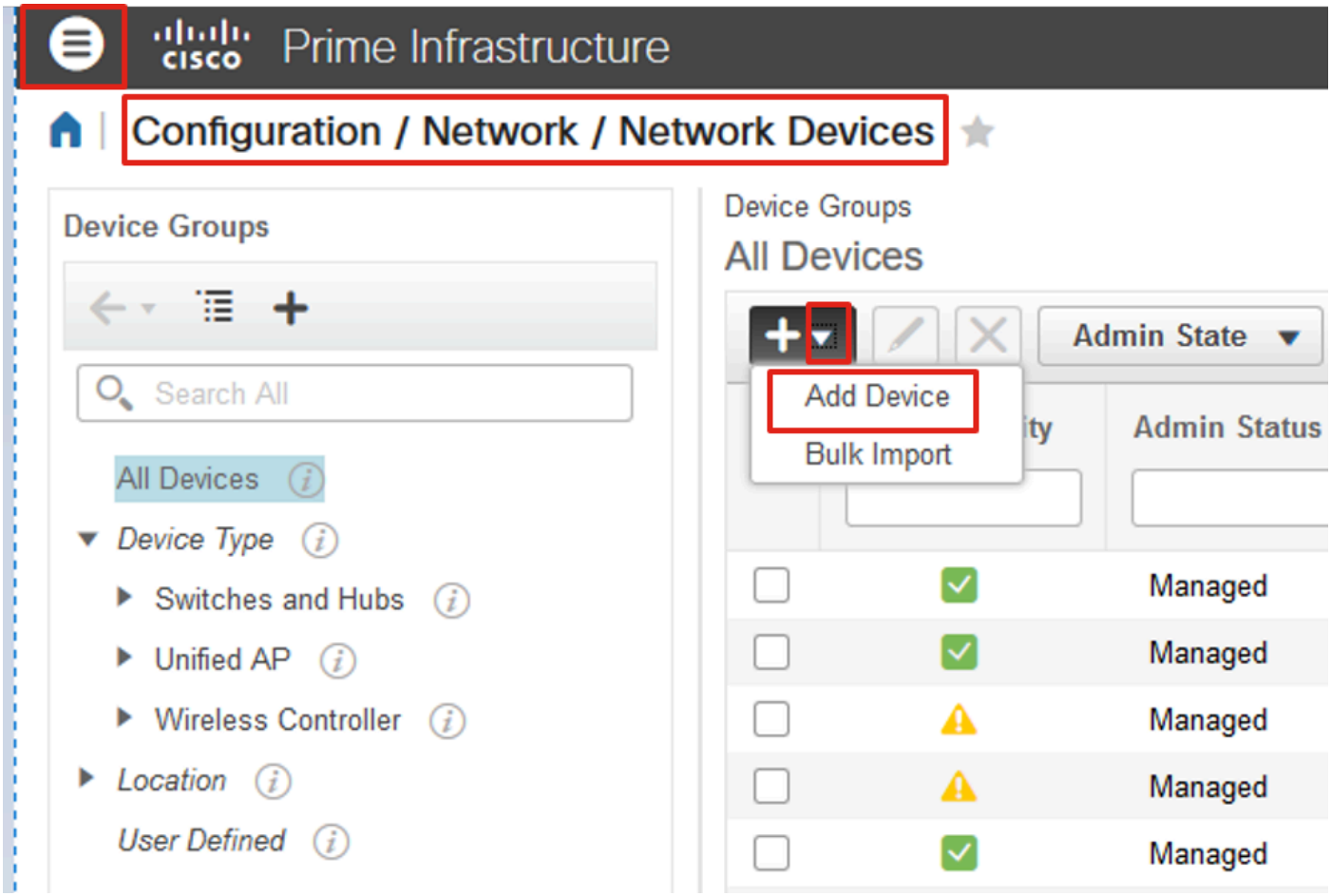


CLI:

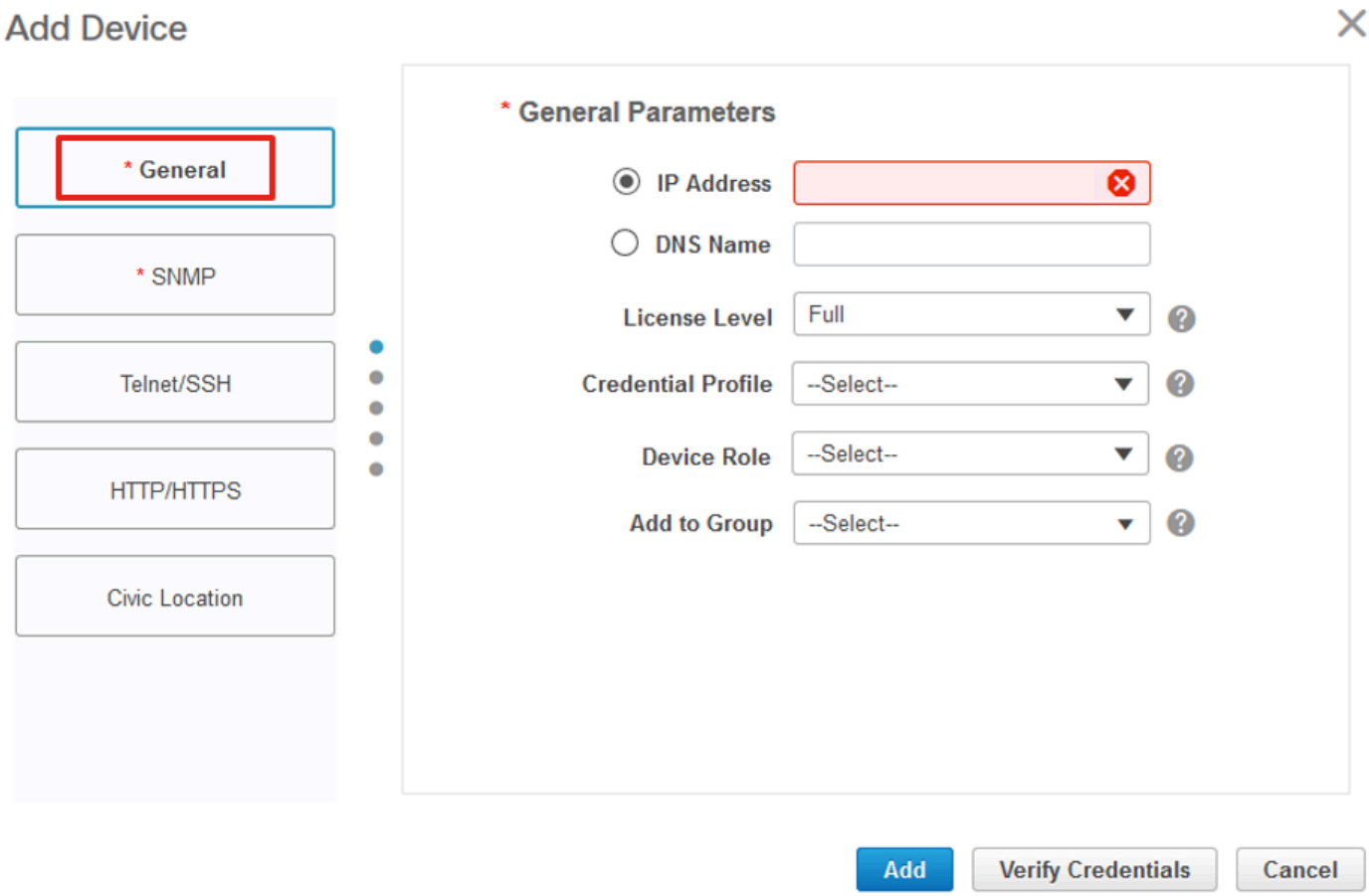
```
For SNMPv2 community strings
# show run | sec snmp

For SNMPv3 user
# show user
```

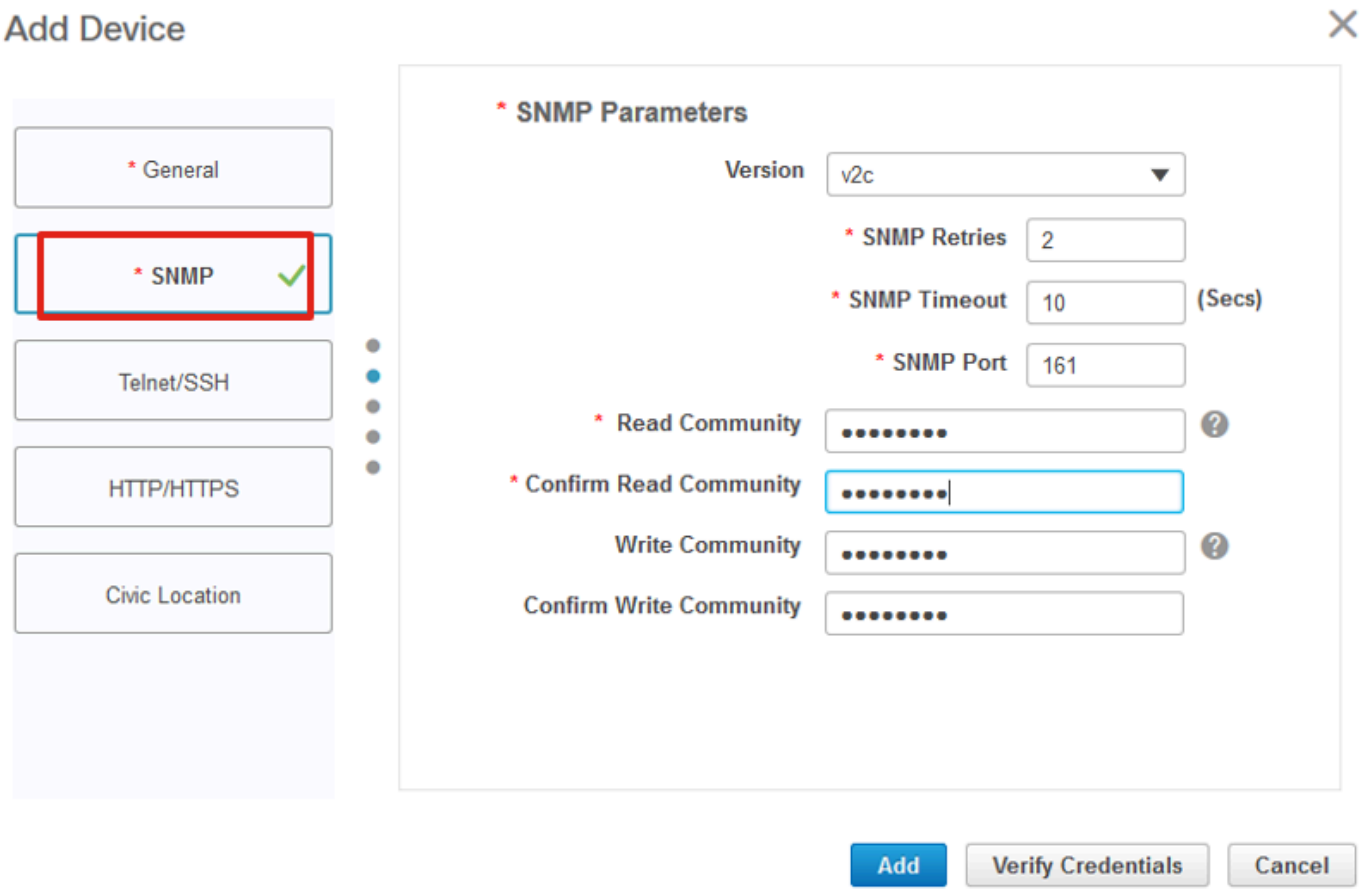
Step 4. On Prime Infrastructure GUI, navigate to **Configuration > Network: Network Devices,** click on the drop-down beside + and choose **Add Device.**



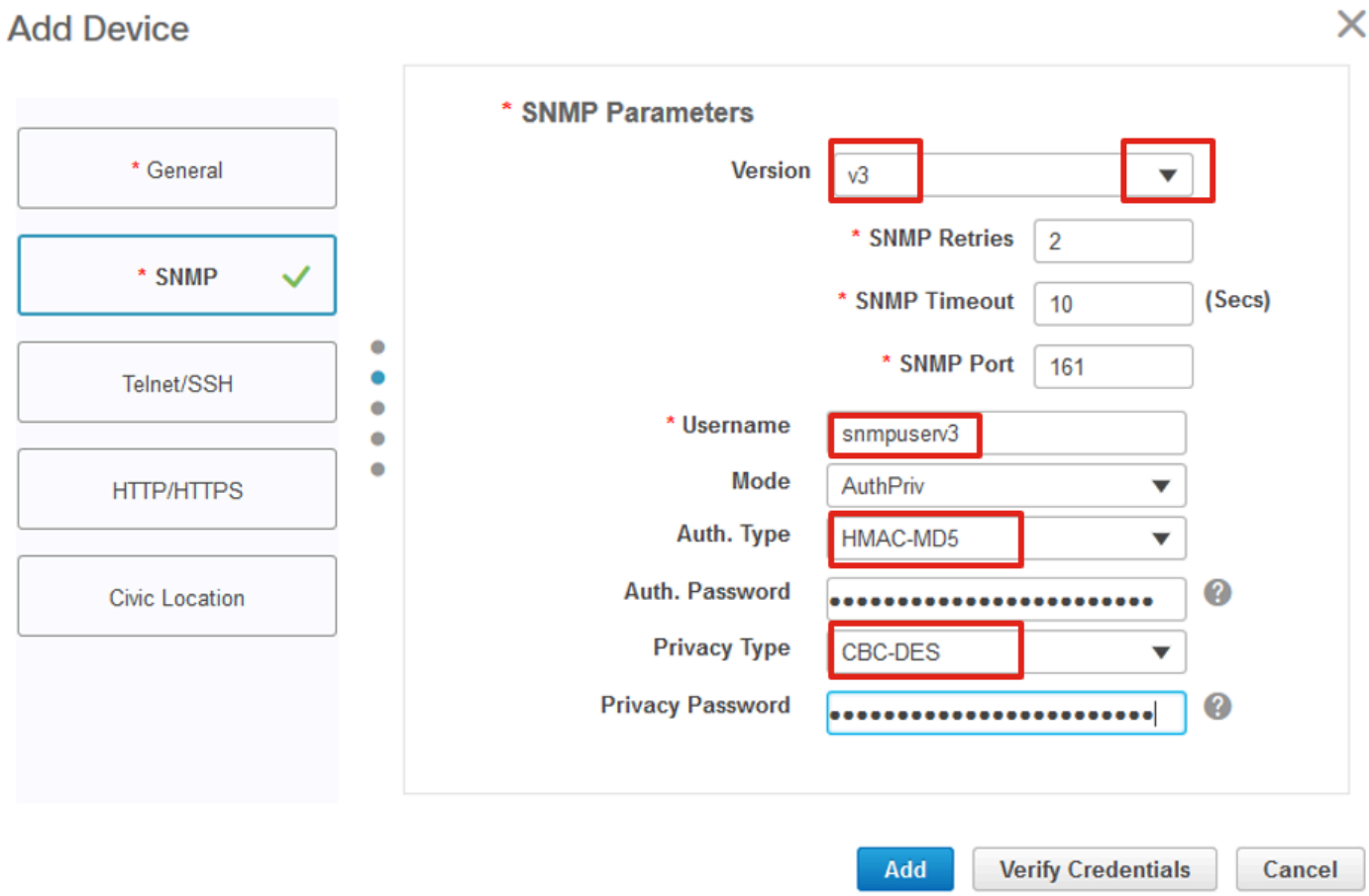
Step 5. On the **Add Device** pop-up, enter the interface ip address on 9800 that is used to establish communication with Prime Infrastructure.



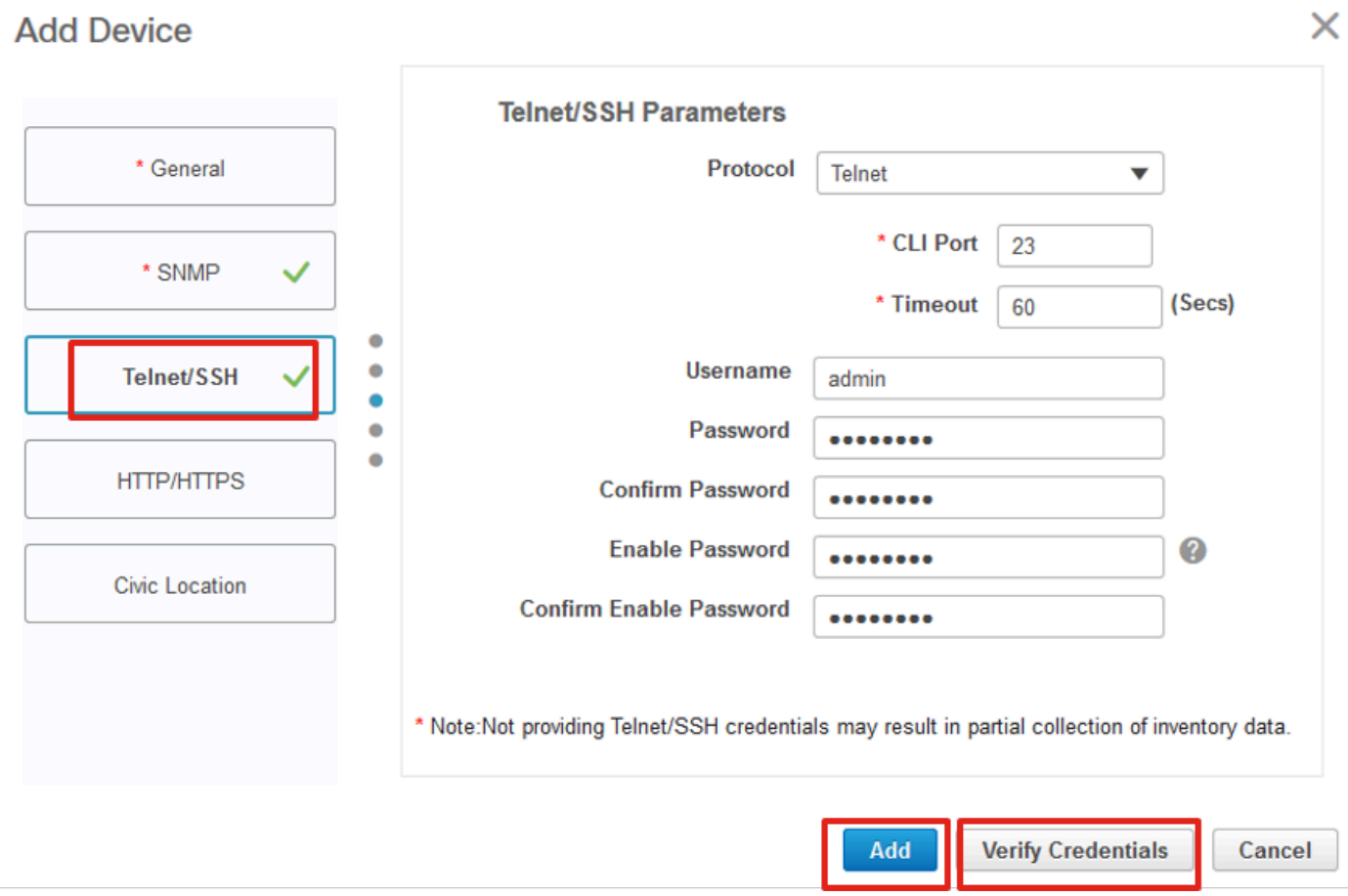
Step 6. Navigate to the **SNMP** tab and provide **SNMPv2 Read-Only and Read-Write Community Strings** configured on C9800 WLC.



Step 7. If using SNMPv3, from the drop-down choose **v3**, and provide the SNMPv3 username. From **Auth-Type** drop-down match the previously configured authentication type and from **Privacy Type** drop-down choose the encryption method configured on C9800 WLC.



Step 8. Navigate to **Telnet/SSH** tab of Add Device, provide the Privilege 15 Username and Password along with Enable Password. Click on **Verify Credentials** to ensure CLI and SNMP credentials work fine. Then click on **Add.**



Verify

Verify Telemetry Status

Step 1. Verify that Netconf is enabled on C9800.

```
#show run | inc netconf
netconf-yang
```

If not present, enter the 'NETCONF configuration on the Cat 9800 WLC' section.

Step 2. Verify the telemetry connection to Prime from the C9800.

```
#show telemetry internal connection
Telemetry connection

Address Port Transport State Profile
--------------------------------------------------------------------
x.x.x.x 20828 cntp-tcp Active
```

Note: x.x.x.x is the ip address of Prime Infrastructure and the state must be Active. If the state is not

Active, refer to the Troubleshoot Section.

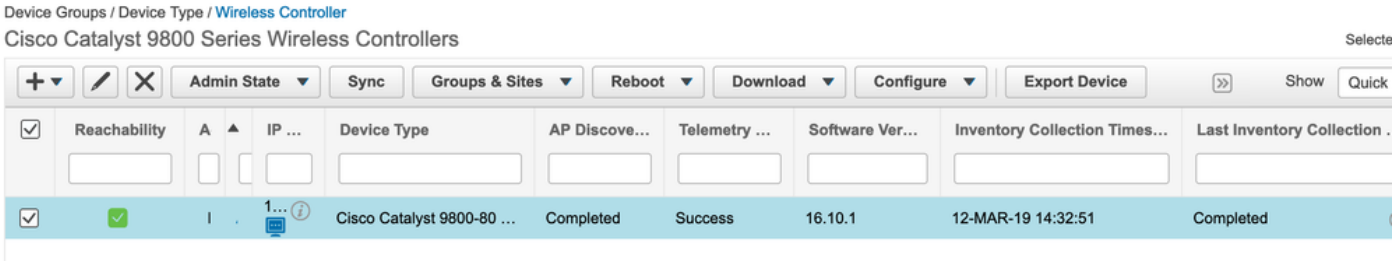
In 17.9, you have to use a slightly different command:

```
9800-17-9-2#show telemetry connection all
Telemetry connections

Index Peer Address              Port  VRF Source Address             State      State Description
----- ------------------------- ----- --- ------------------------- ---------- --------------------
    0 10.48.39.25               25103 0   10.48.39.228              Active     Connection up

9800-17-9-2#
```

Step 3. On Prime Infrastructure, navigate to **Inventory > Network Devices > Device Type: Wireless Controller.**



Step 4. To view the details of the telemetry connection to Prime Infrastructure, run this:

```
#show telemetry internal protocol cntp-tcp manager x.x.x.x 20828
Telemetry protocol manager stats:

Con str                 : x.x.x.x:20828::
Sockfd                  : 79
Protocol                : cntp-tcp
State                   : CNDP_STATE_CONNECTED
Table id                : 0
Wait Mask               :
Connection Retries      : 0
Send Retries            : 0
Pending events          : 0
Source ip               : <9800_IP_ADD>
Bytes Sent              : 1540271694
Msgs Sent               : 1296530
Msgs Received           : 0
```

In 17.9 or later you need to use a different command, the one depicted below.

```
#show telemetry connection all
Telemetry connections
Index Peer Address Port VRF Source Address State State Description
----- ------------------------- ----- --- ------------------------- ---------- --------------------
 1 172.16.0.4 25103 0 172.16.2.44 Active Connection up
```

```
C9800-Classic#show telemetry internal connection <Index> detail
Telemetry protocol manager stats:

Con str : 172.16.0.4:25103:0:172.16.2.44
Sockfd : 116
Protocol : tls-native
State : CNDP_STATE_CONNECTED
Table id : 0
Profile : sdn-network-infra-iwan
Version : TLSv1.2
Wait Mask :
Connection Retries : 0
Send Retries : 0
Pending events : 0
Session requests : 1
Session replies : 1
Source ip : 172.16.2.44
Bytes Sent : 49098323
Msgs Sent : 49918
Msgs Received : 0
Creation time: : Mon Sep 30 16:18:19:535
Last connected time: : Mon Sep 30 16:18:19:587
Last disconnect time: :
Last error: :
Connection flaps: : 0
Last flap Reason: :
Keep Alive Timeouts: : 0
Last Transport Error : No Error
```

Step 5. Verify the telemetry subscription status from C9800 and the fact that they show as 'Valid'.

```
#show telemetry ietf subscription configured
Telemetry subscription brief

ID Type State Filter type
------------------------------------------------------
68060586 Configured Valid transform-na
98468759 Configured Valid tdl-uri
520450489 Configured Valid transform-na
551293206 Configured Valid transform-na
657148953 Configured Valid transform-na
824003685 Configured Valid transform-na
996216912 Configured Valid transform-na
1072751042 Configured Valid tdl-uri
1183166899 Configured Valid transform-na
1516559804 Configured Valid transform-na
1944559252 Configured Valid transform-na
2006694178 Configured Valid transform-na
```

Step 6: The subscription statistics can be viewed per subscription-ID or for all subscriptions using this:

```
#show telemetry internal subscription { all | id } stats
Telemetry subscription stats:

Subscription ID  Connection Info            Msgs Sent  Msgs Drop  Records Sent
------------------------------------------------------------------------------
865925973        x.x.x.x:20828::      2          0          2
634673555        x.x.x.x:20828::      0          0          0
538584704        x.x.x.x:20828::      0          0          0
1649750869       x.x.x.x:20828::      1          0          2
750608483        x.x.x.x:20828::      10         0          10
129958638        x.x.x.x:20828::      10         0          10
1050262948       x.x.x.x:20828::      1369       0          1369
209286788        x.x.x.x:20828::      15         0          15
1040991478       x.x.x.x:20828::      0          0          0
1775678906       x.x.x.x:20828::      2888       0          2889
1613608097       x.x.x.x:20828::      6          0          6
1202853917       x.x.x.x:20828::      99         0          99
1331436193       x.x.x.x:20828::      743        0          743
1988797793       x.x.x.x:20828::      0          0          0
1885346452       x.x.x.x:20828::      0          0          0
163905892        x.x.x.x:20828::      1668       0          1668
1252125139       x.x.x.x:20828::      13764      0          13764
2078345366       x.x.x.x:20828::      13764      0          13764
239168021        x.x.x.x:20828::      1668       0          1668
373185515        x.x.x.x:20828::      9012       0          9012
635732050        x.x.x.x:20828::      7284       0          7284
1275999538       x.x.x.x:20828::      1236       0          1236
825464779        x.x.x.x:20828::      1225711    0          1225780
169050560        x.x.x.x:20828::      0          0          0
229901535        x.x.x.x:20828::      372        0          372
592451065        x.x.x.x:20828::      8          0          8
2130768585       x.x.x.x:20828::      0          0          0
```

Troubleshoot

Troubleshooting on Prime Infrastructure

- The first thing to check on Prime infrastructure is the IP address and interfaces. Prime Infrastructure does not support dual-home and does not listen for telemetry on its second port.
- The IP address of the WLC that you add in Prime Infrastructure must be the IP address used as the 'wireless management interface'. Prime Infrastructure IP address must be reachable from that wireless management interface on the controller side.
- If using Service port (gig0/0 on appliances) for discovery, WLC and APs show up in the Managed state in Inventory but telemetry for WLC and associated Access Points does not work.
- If you see the telemetry status to be a 'success' on Prime Infrastructure but the AP count is 0, it could be that Prime Infrastructure can reach out to the WLC on port 830 but the controller cannot reach back the Prime Infrastructure on port 20830.

For any SNMP issues or device configuration issues, collect these logs from Prime Infrastructure:

```
cd /opt/CSCOlumos/logs/
```

```
[root@prime-tdl logs]# ncs-0-0.log

Tdl.logs
```

For Telemetry/coral issues, the first thing is to check the Coral status:

```
shell

cd /opt/CSCOlumos/coralinstances/coral2/coral/bin

./coral version 1

./coral status 1

./coral stats 1
```

If all is well, collect these logs from the prime coral logs folder.

Note: Depending on the Prime Infrastructure version and the amount of Cisco IOS XE version it supports, there can be several Coral instances on Prime Infrastructure. Check releases notes for more details such as: https://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/3-7/release/notes/bk_Cisco_Prime_Infrastructure_3_7_0_Release_Notes.html

---

Step 1.

```
cd /opt/CSCOlumos/coral/bin/

[root@prime-tdl bin]# ./coral attach 1

Attached to Coral instance 1 [pid=8511]

Coral-1#cd /tmp/rp/trace/

Coral-1#ls

Collect the  “Prime_TDL_collector_R0-”* logs
```

```
Coral-1# cd /tmp/rp/trace/
Coral-1# btdecode P* > coralbtlog.txt
Coral-1# cat  coralbtlog.txt
```

These logs can also be found in this directory:

* The decoded trace files are available in the path**/opt/CSCOlumos/coralinstances/coral2/coral/run/1/storage/harddisk**
* **ade# cd /opt/CSCOlumos/coralinstances/coral2/coral/run/1/storage/harddisk**
* **ade# cp coraltrace.txt /localdisk/defaultRepo**

Step 2. To enable Coral in debug mode, debug level needs to be set in **debug.conf** file.

Either from within the container:

```
echo "rp:0:0:tdlcold:-e BINOS_BTRACE_LEVEL=DEBUG;" > /harddisk/debug.conf
```

Or on Prime 3.8, Coral service can be restarted outside of the container using:

```
"sudo /opt/CSCOlumos/coralinstances/coral2/coral/bin/coral restart 1"
```

If the restart doesn’t help these can be used to wipe the coral instance and start it smoothly:

```
sudo /opt/CSCOlumos/coralinstances/coral2/coral/bin/coral stop 1
sudo /opt/CSCOlumos/coralinstances/coral2/coral/bin/coral purge 1
sudo /opt/CSCOlumos/coralinstances/coral2/coral/bin/coral start 1
```

Restart Coral, this is mandatory. You can leave the coral instance if you type 'Exit' then:

```
./coral/bin/coral restart 1
```

Note: On Prime 3.8, Coral service can be restarted outside of container using 'sudo /opt/CSCOlumos/coralinstances/coral2/coral/bin/coral restart 1'

If you need to decode Coral log files, you can decode them inside the Coral container with:

```
btdecode Prime_TDL_collector_*.bin
```

Note: After enabling debug level of Coral, restarting Coral is mandatory.

Troubleshooting on Catalyst 9800 WLC

To monitor the configuration pushed by Prime Infra to the C9800 WLC, you can run an EEM applet.

```
#config terminal
#event manager applet catchall
 #event cli pattern ".*" sync no skip no
 #action 1 syslog msg "$_cli_msg"
```

Delete All the Telemetry Subscription from the WLC Configuration

There can be times when you want to unconfigure all telemetry subscriptions configured on the WLC. This can be done simply with these commands:

```
WLC#term shell
WLC#function removeall() {
for id in `sh run | grep telemetry | cut -f4 -d' '`
do
conf t
no telemetry ietf subscription $id
exit
done
}
WLC#removeall
```

To enable traces:

```
# debug netconf-yang level debug
```

To verify:

```
WLC#show platform software trace level mdt-pubd chassis active R0 | inc Debug

pubd                            Debug

WLC#show platform software trace level ndbman chassis active R0 | inc Debug

ndbmand                         Debug
```

To view the trace outputs:

```
show platform software trace message mdt-pubd chassis active R0

show platform software trace message ndbman chassis active R0
```

Check for Subscription ID for AP Information

Click on **DB Query**. Navigate tohttps://<Prime_IP>/webacs/ncsDiag.do.

Choose *from **ewlcSubscription** where OWNINGENTITYID like '%Controller_IP' and CLASSNAME='UnifiedAp'.

From WLC:

Verify that the subscription ID is sending information and no drops on the cntp counters.

```
show tel int sub all stats

show telemetry internal protocol cntp-tcp connector counters drop

show telemetry internal protocol cntp-tcp connector counters queue

show telemetry internal protocol cntp-tcp connector counters rate

show telemetry internal protocol cntp-tcp connector counters sub-rate

show telemetry internal protocol cntp-tcp connector counters reset
```



Note: The 9800 WLC supports 100 telemetry subscription before 17.6 and up to 128 subscriptions after 17.6 (as recent release of Catalyst center can use more than 100 subscriptions.

Migration from PI to Cisco Catalyst Center

C9800 can not be simultaneously managed by both PI and Cisco Catalyst Center. If there is a plan to move to Catalyst Center as a network management solution, C9800 needs to be removed from Prime Infrastructure before adding it to Catalyst Center. When C9800 is removed/deleted from PI 3.5, all the configuration that was pushed to C9800 at the time of inventory by PI does not get rolled back and these need to be manually deleted from the system. Specifically, the subscription channels established for C9800 WLC to publish streaming telemetry data do not get removed.

To identify this specific configuration:

```
#show run | sec telemetry
```

To remove this configuration, run the **no** form of the command:

```
(config) # no telemetry ietf subscription <Subscription-Id>
Repeat this CLI to remove each of the subscription identifiers.

(config) # no telemetry transform <Transform-Name>
Repeat this CLI to remove each of the transform names
```



Note: If you manage the 9800 controller with both Catalyst Center and Prime Infrastructure, the Catalyst Center inventory compliance fails expectedly because of Prime management.

In recent releases, both Prime Infrastructure and Catalyst Center can use too many telemetry subscriptions for the WLC for both servers to manage the 9800 simultaneously. You therefore cannot manage the 9800 with both Catalyst Center and Prime Infrastructure and have telemetry and statistics working. Migration from PI to Catalyst Center must therefore happen as fast as possible because Catalyst Center is not able to have telemetry data from the 9800 as long as Prime Infrastructure is managing the 9800 controller.