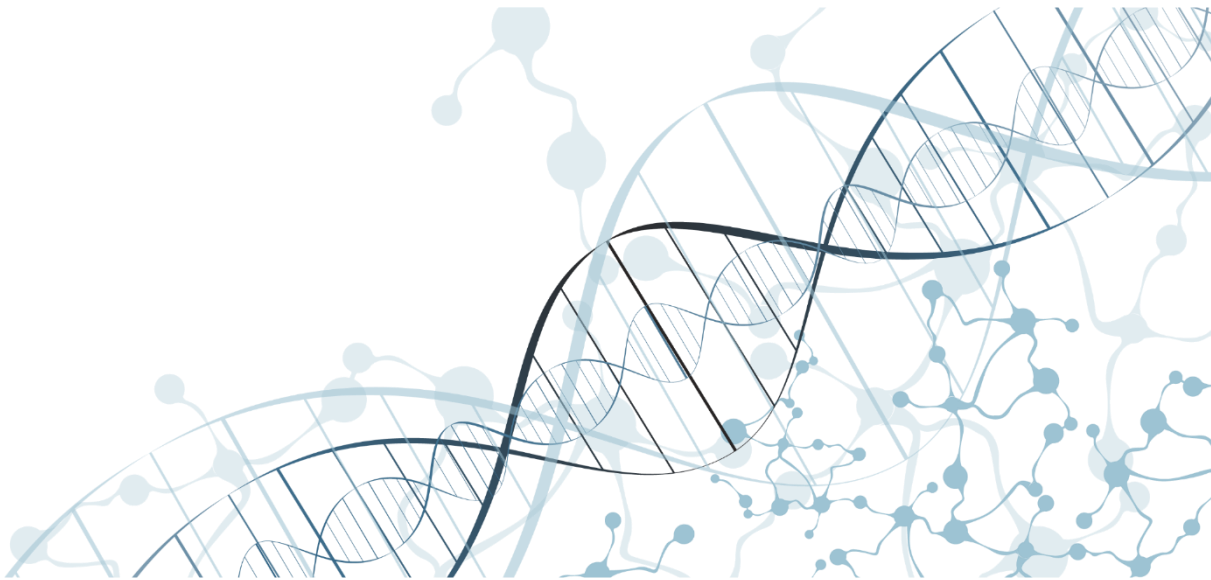


Cisco 1800S Sensor Deployment Guide



Americas Headquarters

Cisco Systems, Inc. 170 West Tasman Drive

San Jose, CA 95134-1706 USA

<http://www.cisco.com>

Tel: 408 526-4000 800

553-NETS (6387)



Table of Contents

Overview of Cisco 1800S Sensor	3
Recommended Software Requirements	3
Prerequisite: Install Sensor Packages from Cisco DNA Center	3
Cisco 1800S Sensor Hardware	4
Sensor Deployment: Design and Installation	6
Software Setup Processes	7
Sensor Data Flow	9
Provision Sensors	9
Preparation: Network Connectivity Between Sensors and Cisco DNA Center	10
Wired Backhaul Environment	10
Day-0, Factory-Installed SSID Between Sensor and Cisco AP	10
Cisco DNA Center Discovery from Sensor	14
DHCP Option 43	14
DNS-Based Cisco DNA Center Discovery	17
Cisco DNA Provisioning Through CLI	18
Connect Your Sensor to the Network	19
Persistent Wireless Backhaul	19
Create a Sensor Backhaul Profile in Cisco DNA Center	20
Provision the Sensor: Claim the Device	21
Upgrade the Sensor Software in 8 Steps	24
Place the Sensor on the Floor Map	26
Manage Sensors	27
Create a Sensor Test Template	28
Monitor Sensor Health	39
Wireless Sensor Dashboard	39
Sensor 360	42
Sensor Global Issues	44
Troubleshooting	44
Sensor Command Line Interface	44
Event Log and Sensor Support Bundle	45
Reset Sensor Configuration	46
Show Heartbeat Status	46
PNP related CLIs (useful during PnP provisioning phase)	49
Detailed Troubleshooting Commands Output	49

Useful Links.....49

Overview of Cisco 1800S Sensor

Today's enterprise networks are evolving. Enterprise WLAN has become mission critical as more companies migrate to wireless connectivity for their key use cases.

As wireless networks grow, especially in remote facilities where IT professionals are not always onsite, it's important to quickly identify and resolve potential connectivity issues before connectivity degradation occurs.

To address these issues, Cisco has created Cisco DNA Assurance and the Cisco 1800S Sensor. The Cisco DNA Assurance platform has three components: wireless performance analytics, real-time client troubleshooting, and proactive health assessment. Using a sensor, a device can function like a WLAN client, associating and identifying client connectivity issues in the network in real time without requiring an onsite IT technician.

This document covers the standalone Cisco 1800S Sensor.

Recommended Software Requirements

- Cisco DNA Center Release 1.3.3.0
- Cisco 1800S Sensor Release 1.3.3.0

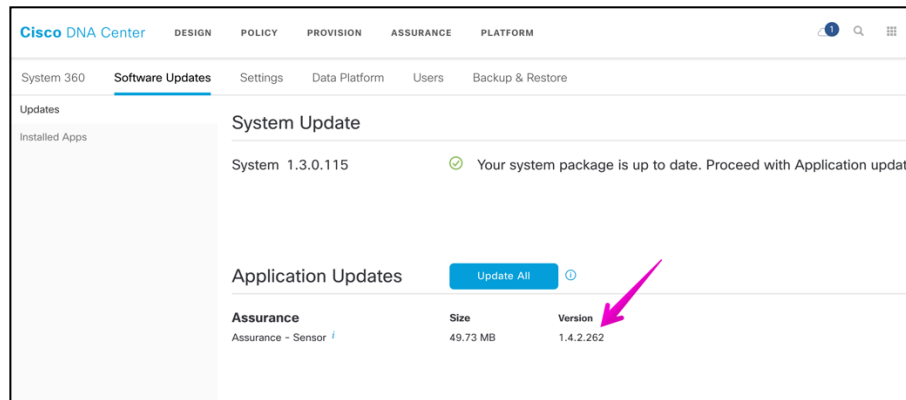
Sensor Suggested Software Release	Cisco DNA Center Software Release
1.3.3.0	Suggested for Cisco DNA Center 1.3.3.x
1.3.1.2	Suggested for Cisco DNA Center 1.3.1.2 or later 1.3.1.x
8.8.263.0	Suggested for Cisco DNA Center 1.3.0.3 or earlier (example: 1.2.x)

This document is based on the recommended Cisco 1800S Sensor Release 1.3.3.0 software environment. Some software features are not supported on earlier software releases.

Prerequisite: Install Sensor Packages from Cisco DNA Center

Cisco DNA Center provides the option to download separate sensor packages called **Assurance - Sensor** and **Automation - Sensor**. You can download and install these packages on top of the base Cisco DNA Center software. To install the sensor packages, log in to Cisco DNA Center and click the gear icon in the top-right corner. Click **System Settings** and then click the **Software Updates** tab.

Assurance Sensor Packages



Cisco 1800S Sensor Hardware

The Cisco 1800S Sensor is a small form factor, dedicated sensor that can be powered in many different ways through a small sliding module that inserts into the sensor.

Cisco 1800S Sensor

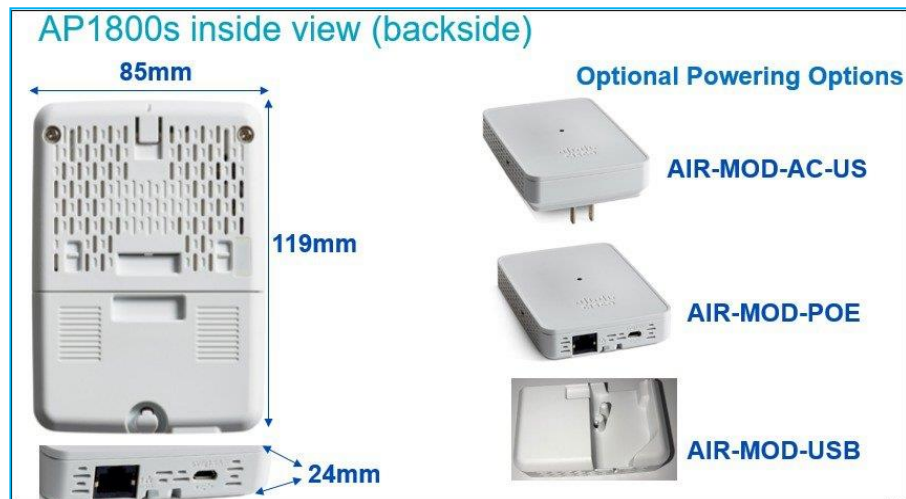
Purpose-built wireless sensor for Cisco DNA Assurance



- 2x2 with 2 spatial streams
- 802.11ac wave 2 sensor
- Multiple power options:
 - 802.3af PoE module
 - Micro-B USB type connector (2.5 amperes/5 volts)
 - AC wall socket adapter
- Small form factor (WxLxH):
- 3.25" x 4.75" x 0.75"

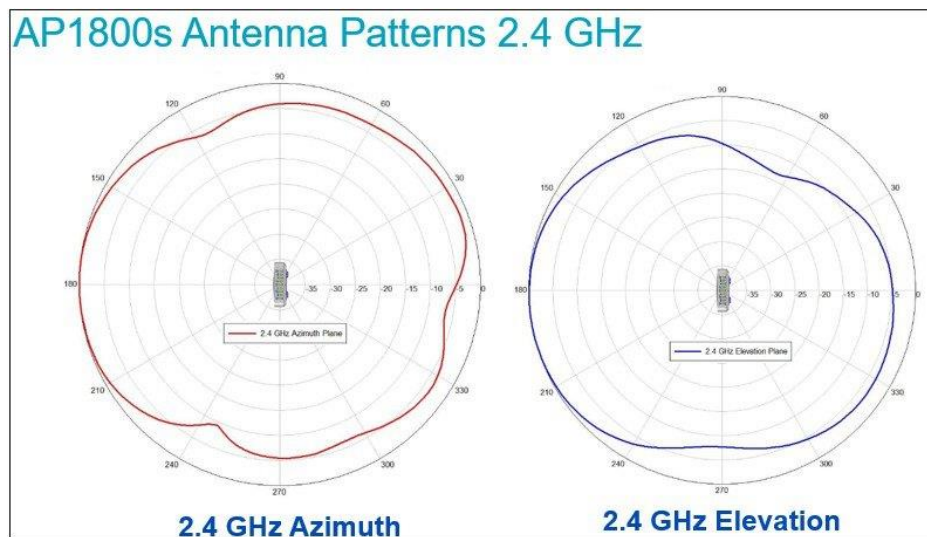
Without a power over Ethernet (PoE) module, power can be supplied from a local 2.5 ampere/5-volt USB port, using a micro-USB Type-B connector. (There is USB Type-C connector, but it is dedicated for the PoE module connection.) Additionally, there are modules that allow for a direct AC power supply, as well as PoE operation.

Cisco 1800S Sensor - Backside View



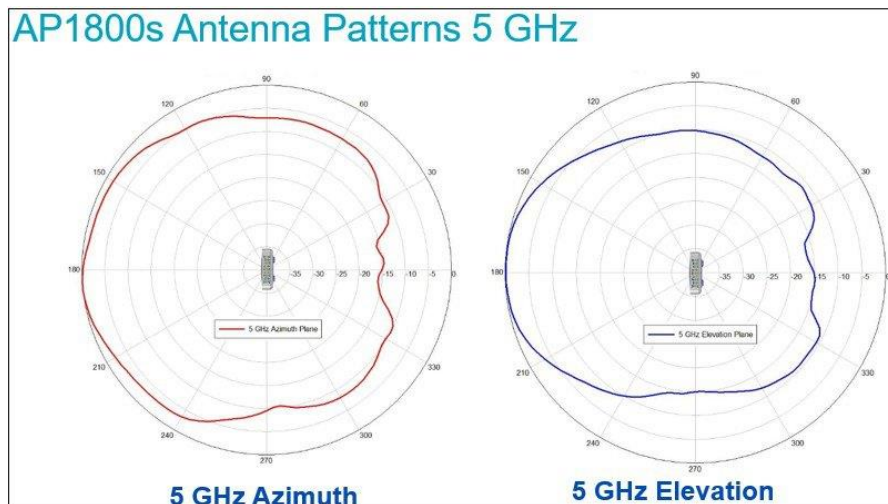
The following figures show the antenna system on the sensor.

Cisco 1800S Sensor - Antenna Pattern 2.4 GHz



Cisco 1800S Sensor - Antenna Pattern 5 GHz

AP1800s Antenna Patterns 5 GHz



Cisco 1800S Sensor and Accessory Product IDs (PIDs)

Name	Product ID
Cisco 1800S Sensor	AIR-1800S-x-K9
PoE with 1 G Ethernet Module	AIR-MOD-SPOE
USB Adapter Power Module – US Plug Only	AIR-MOD-USB-US=
USB Adapter Power Module – Rest of World (includes bag of 5 international plugs)	AIR-MOD-USB-RW=
Wall Mount Bracket Kit	AIR-AP-BRACKET-NS
Cisco 1800S Console Cable	AIR-CONADPT=
AC Adapter Power Module	AIR-MOD-AC-US/CH/EU/IN/UK

Sensor Deployment: Design and Installation

The ideal deployment location for sensor is wall-mount with desktop height, between 22 to 47 inches from the floor.

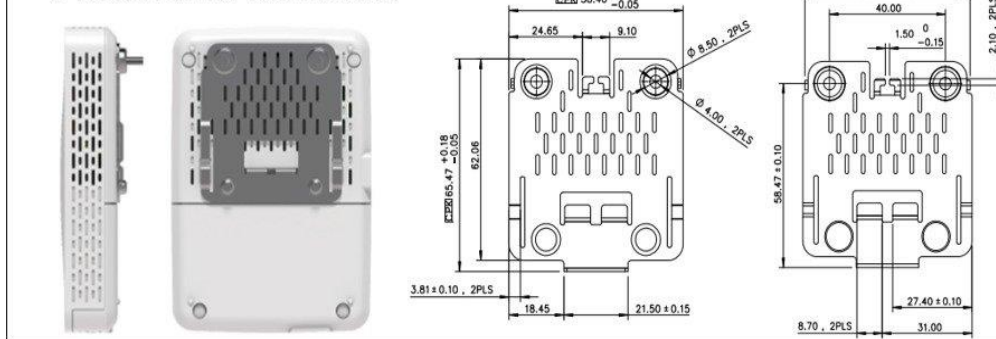
Due to its small size, the sensor uses a specially designed metal-based wall mount bracket, part number AIR-AP-BRACKET-NS.

Cisco 1800S Sensor - Mounting

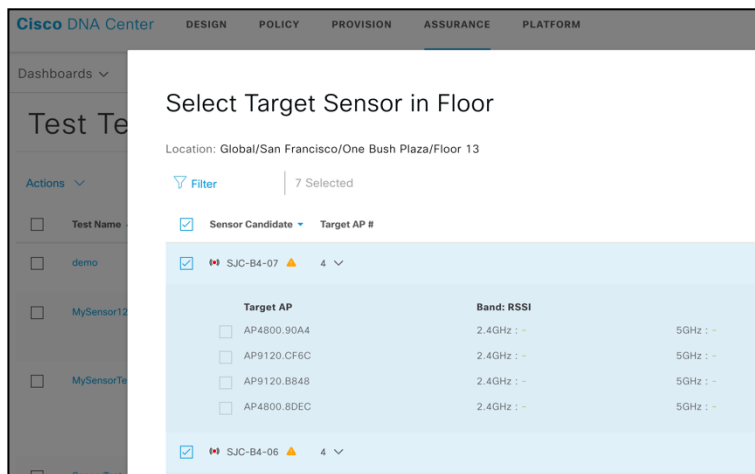
Installation – AIR-AP-BRACKET-NS

■ Mounting:

➤ New small wall-mount bracket



Because the sensor simulates a wireless client environment, the sensor can be configured to associate to the nearest AP based on RSSI. The test target AP can extend up to 5 APs. For example, if a single floor has 40 APs and the administrator wants to test all 40 APs, he or she must deploy at least eight sensors. However, the sensor's target AP selection process is dynamic, selecting up to the top five highest RSSI APs. Administrators can manually assign target APs per sensor.



Software Setup Processes

Sensor deployment involves the following steps.

Sensor Deployment Steps

Step1. Plan

- Determine deployment size, scale
- Determine deployment location
- Prepare Test servers
- Configure DHCP or DNS server
- Setup Wired network connectivity between sensor and Cisco DNA Center
- Determine powering option for sensor (PoE or USB or Wall Socket)
- Order Sensor
- Create Sensor PnP Profile for Wireless Sensor
- Create Sensor Test Template

Step2. Deploy

- Install Sensors
- Sensor connected to Cisco DNA Center
- If DHCP/DNS is not configured use manual ssh option to configure Cisco DNA Center in Sensor
- Provision Sensor via PnP Claim
- Verify Sensor Claimed condition from Sensor List page
- Download latest Sensor software
- Upgrade Sensor Image software if it's needed
- Manage Sensor HW (LED control, Name change, SSH control)
- Assign specific Test Template to specific Sensor (Optional)

Step3. Operate

- Observe Sensor Test result via Sensor Dashboard, Sensor 360
- Detect Network failure from Sensor Issues
- Troubleshoot Sensor if there is suspicious, erratic result using Sensor 360-page Event Log section
- Plan on additional Sensor Location

Mandatory Step

Optional Step

Planning (Process-based)

Network Operation

Cisco DNA Center Operation

Step 1. Plan (Day 0)

1. Plan how many sensors will be deployed per location, per floor.
2. Decide the sensor installation points.
3. Create a sensor PnP profile for sensor provisioning (optional for wireless sensors).
4. Prepare sensor test target servers (AAA, servers, email, FTP, and so on).
5. Create a sensor test template in Cisco DNA Center.
6. Configure a DHCP or DNS server for Cisco DNA Center information.
7. Set up wired network connectivity between the sensor connected port and Cisco DNA Center (manual; required for wired sensors).
8. Complete wired PoE cabling for the sensor connection (part of the installation work for wired sensors).

Step 2. Deploy (Day 1)

1. Install sensors in the predetermined location.
2. Configure the sensors to learn the Cisco DNA Center IP address via DHCP or DNS.
3. Connect the sensors to Cisco DNA Center via http.
4. Provision the sensors via a PnP claim.
5. Verify the Sensor Claimed condition from the Sensor List page.
6. Download the latest sensor software via Golden Image marking.
7. Upgrade the sensor image software, if required.
8. Manage the sensor hardware (LED control, name change, SSH control).
9. Assign specific test templates to specific sensors (if you want to have manual assignment).

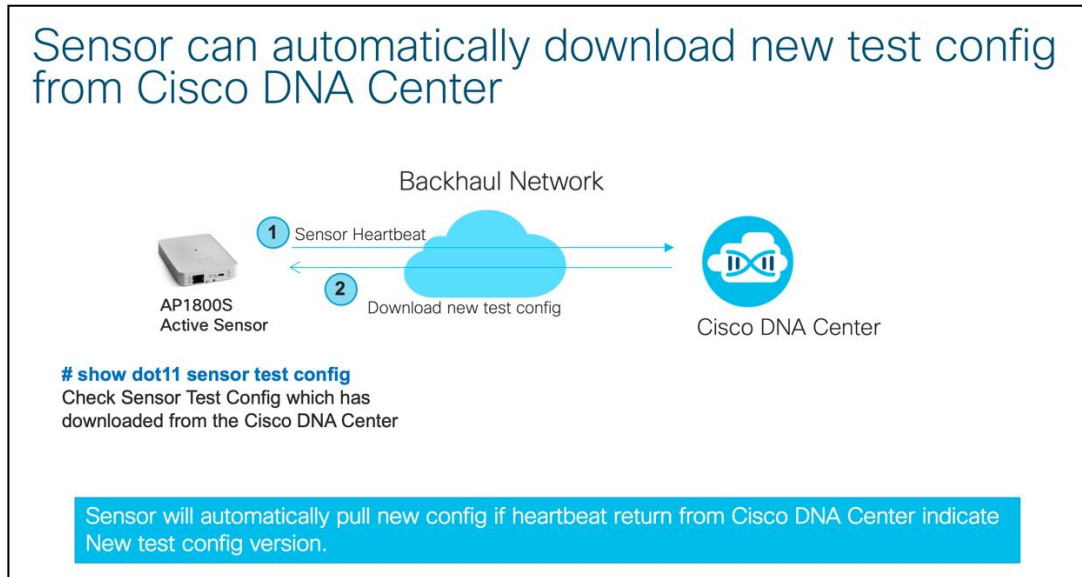
Step 3. Operate (Day 2)

1. Observe the sensor test results via the sensor dashboard, **Sensor 360**.
2. If you see suspicious, erratic results, troubleshoot the sensors using the **Sensor 360** page, **Event Log** section.

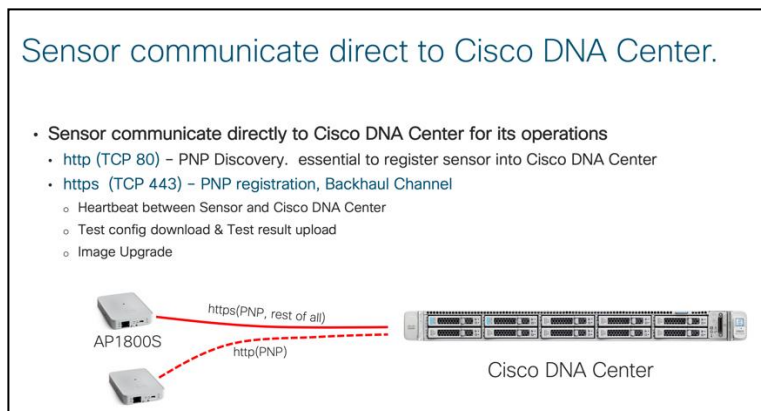
Sensor Data Flow

The sensor receives the test suite configuration directly from Cisco DNA Center.
Sensor test results traverse directly from the sensor to Cisco DNA Center.

Sensor Test Config Data Flow



Network Port Between Sensor and Cisco DNA Center



Provision Sensors

The sensor is not an AP. It's designed as a dedicated sensor, simulating wireless client behavior. The sensor does not join the wireless controller because it operates independently from the wireless controller. Instead, the sensor depends on Cisco DNA Center for provisioning, configuration, operation, monitoring, and upgrade. The sensor automatically connects to Cisco DNA Center by leveraging the DHCP Option 43 field as part of DHCP OFFER from the DHCP server. DHCP Option 43 contains a string of parameters that the sensor needs to find Cisco DNA Center. One of these parameters is the IP address of Cisco DNA Center. If the sensor fails to receive the IP address of Cisco DNA Center from DHCP, the sensor tries a DNS query for the designated hostname, PNPSEVER. The last resort is manual CLI input via console or SSH.

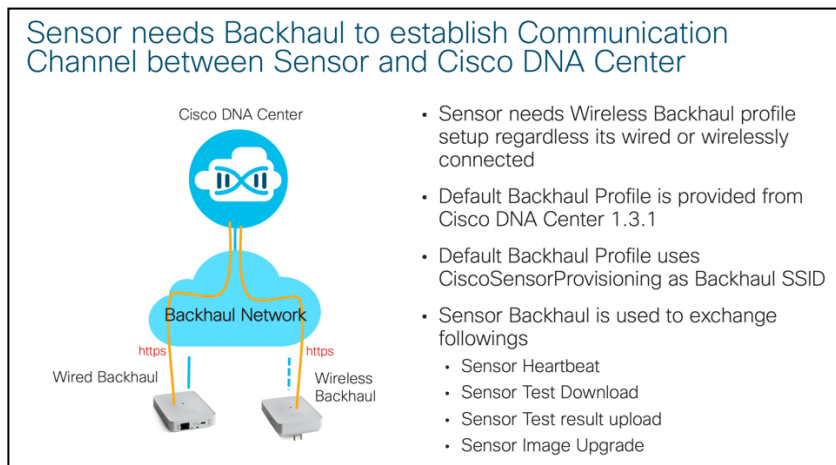
Preparation: Network Connectivity Between Sensors and Cisco DNA Center

For correct sensor operation, direct network connectivity is required between the sensors and Cisco DNA Center. This network connectivity from the sensor is called the *backhaul interface*. Sensors use the backhaul interface to communicate with Cisco DNA Center, which requires direct connectivity using http (TCP 80) and https (TCP 443). Proxy is not supported.

Sensors support two types of backhaul interfaces: *wired* and *wireless*.

The wired backhaul interface is supported via the PoE module. The wireless backhaul interface shares the same radio interface with the wireless testing radio interface.

Sensor Backhaul Network types



Wired Backhaul Environment

When the sensor is equipped with a PoE module (AIR-MOD-POE=), the sensor can receive power from the PoE switch port using the 802.3af standard. Sensors can also establish connection to Cisco DNA Center via this wired PoE interface and use the wired IP address to communicate with Cisco DNA Center. This type of sensor network configuration is called *wired backhaul*. If the sensor does not receive an IP address for the wired interface, the sensor switches to wireless backhaul to search for and connect to Cisco DNA Center. For the wireless backup connection, the administrator must assign a sensor profile during the sensor PnP claiming step. In an SDA/fabric environment, the fabric edge that serves the sensor connection must have MTU 1550 configured. The recommended MTU size is 9200.

Day-0, Factory-Installed SSID Between Sensor and Cisco AP

Out of the box, the sensor must be able to associate and communicate with Cisco DNA Center. This is relatively easy if the sensor has a wired Ethernet connection. If the sensor does not have an Ethernet connection and only has power to boot up, the sensor cannot connect to any AP.

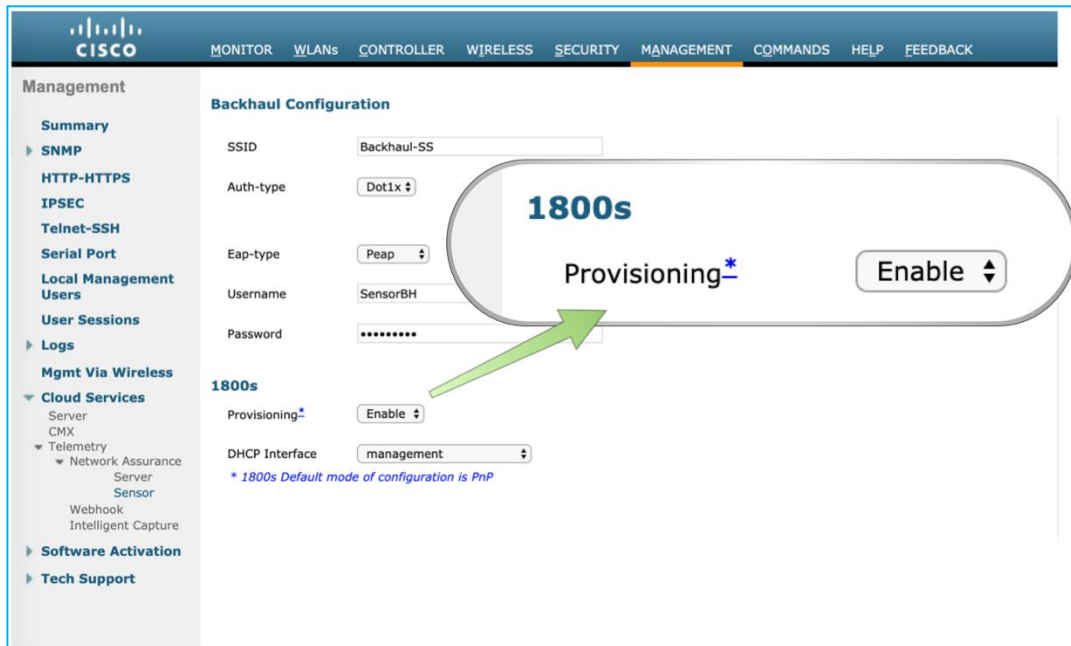
To solve this problem, the AP and sensor use a factory installed SSID named *CiscoSensorProvisioning*. This SSID is known to both the wireless controller and the sensor from a factory shipment level.

The CiscoSensorProvisioning SSID is designed to connect the sensor to Cisco DNA Center.

The CiscoSensorProvisioning SSID uses 802.1x/EAP-TLS as its sensor device authentication and encryption mechanism. The wireless controller enables the CiscoSensorProvisioning SSID and assigns it within the first 16 WLAN SSIDs.

The CiscoSensorProvisioning SSID can be used in FlexConnect environments, but the CiscoSensorProvisioning SSID itself can only be used in a central switching environment.

Cisco 1800S Sensor Day 0 Provisioning Configuration - WLC



The wireless controller enables a series of configurations to enable the wireless provisioning SSID for the sensor.

1. Create a backhaul SSID with the predefined *CiscoSensorProvisioning* name.

- This is a special purpose, hidden SSID that is designed to connect to the sensor wirelessly.
- The sensor can connect to the Cisco AP and use it to reach Cisco DNA Center.
- The CiscoSensorProvisioning SSID uses any available WLAN ID from among the first 16 WLAN IDs. If WLAN IDs 1 to 16 are all in use, CiscoSensorProvisioning SSID creation fails.

In the preceding figure, you can disregard the “Backhaul Configuration” section; you don’t need to configure backhaul for the sensor.

2. Enable the local EAP server with EAP-TLS to authenticate the sensor’s embedded certificate.

Cisco 1800S Sensor Provisioning SSID

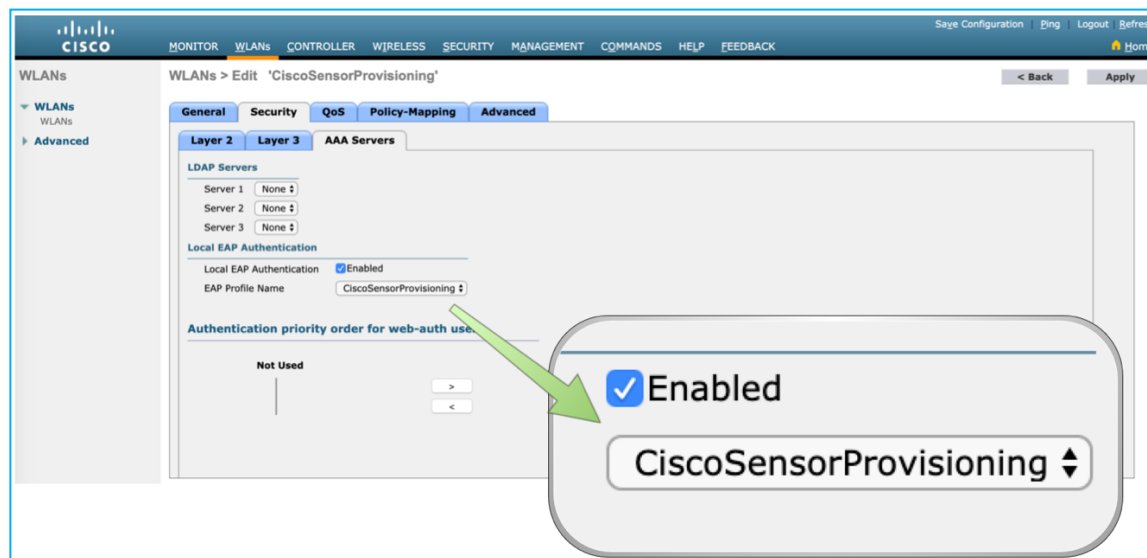
The screenshot shows the Cisco WLC WLANs page. The table lists various WLANs with columns for WLAN ID, Type, Profile Name, WLAN SSID, Admin Status, and Security Policies. The row for WLAN ID 5, which is the CiscoSensorProvisioning SSID, is highlighted with a red box.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	ss-dot1x	ss-dot1x	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	ss-open	ss-open	Enabled	None
3	WLAN	ss-psk	ss-psk	Enabled	[WPA2][Auth(PSK)]
4	WLAN	ss-alpha	ss-alpha	Enabled	[WPA2][Auth(802.1X)]
5	WLAN	CiscoSensorProvisioning	CiscoSensorProvisioning	Enabled	[WPA2][Auth(802.1X)]
17	WLAN	ss-corp	ss-corp	Enabled	[WPA2][Auth(802.1X)]

This SSID also enables to a local authentication profile that is created automatically when you enable the CiscoSensorProvisioning SSID for the sensor.

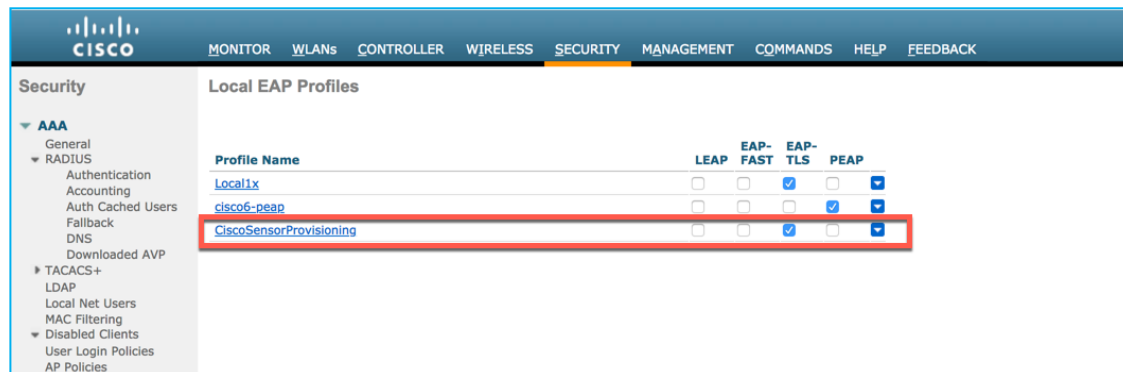
The following screen shots show the SSID and local authentication profile that are created.

Local Authentication Profile Assigned to the CiscoSensorProvisioning SSID



The sensor authenticates with the controller with an in-built device certificate on the sensor with EAP-TLS.

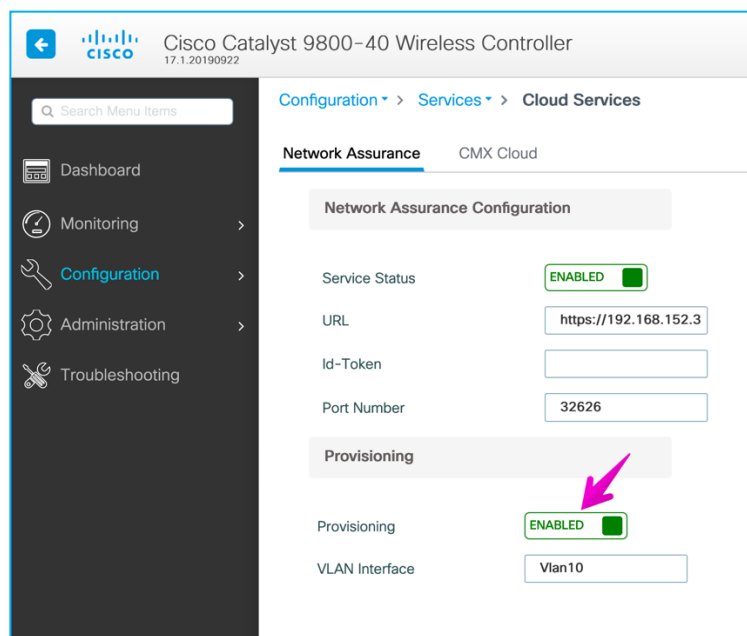
Local Authentication Profile for Cisco 1800S Sensor Provisioning



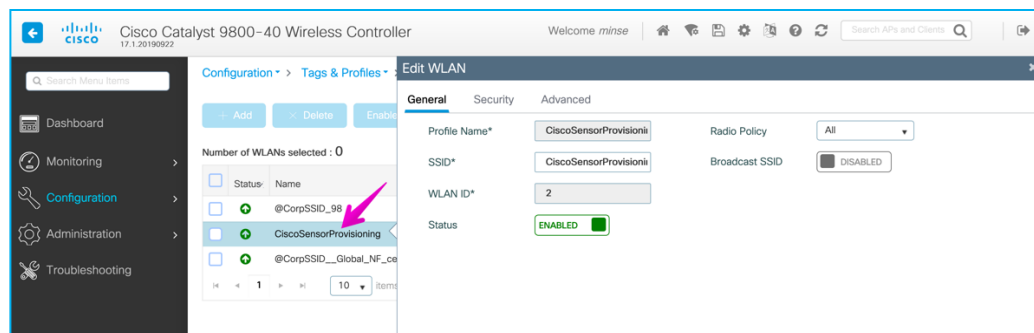
Note: The CiscoSensorProvisioning SSID does not broadcast SSID over the air. It's hidden by default; the sensor can discover and connect to this hidden CiscoSensorProvisioning SSID.

Later, the network administrator can allocate the CiscoSensorProvisioning SSID to various AP groups, making the CiscoSensorProvisioning SSID available only to specific locations.

For Cisco Catalyst 9800 devices, the CiscoSensorProvisioning SSID is enabled from **Configuration > Services > Cloud Services > Network Assurance > Provisioning: ENABLED**.



After provisioning is enabled, the network administrator can view the newly added SSID from **Configuration > Tags & Profile > WLANs**.



Unlike AireOS, the Cisco IOS XE-based Catalyst 9800 allows config changes in the CiscoSensorProvisioning SSID. However, we do not recommend that you change the configuration, because config changes can break compatibility with the sensor.

Cisco DNA Center Discovery from Sensor

First, the sensor must learn the Cisco DNA Center IP address. The network administrator must send the Cisco DNA Center IP address to the sensor by:

1. DHCP Option 43
2. DNS discovery
3. Configuration through the sensor CLI using the console cable (AIR-CONSADPT=) or SSH

DHCP Option 43

The most common method of sending the IP address of Cisco DNA Center to the sensor is by packaging the IP address as part of the DHCP IP addressing process.

The network administrator uses the DHCP Option 43 field to add the Cisco DNA Center IP address. The network administrator enters the following ASCII formatted string into DHCP Option 43 field:

```
5A1N;B2;K4;I<Cisco DNA Center IP Address>;J80
```

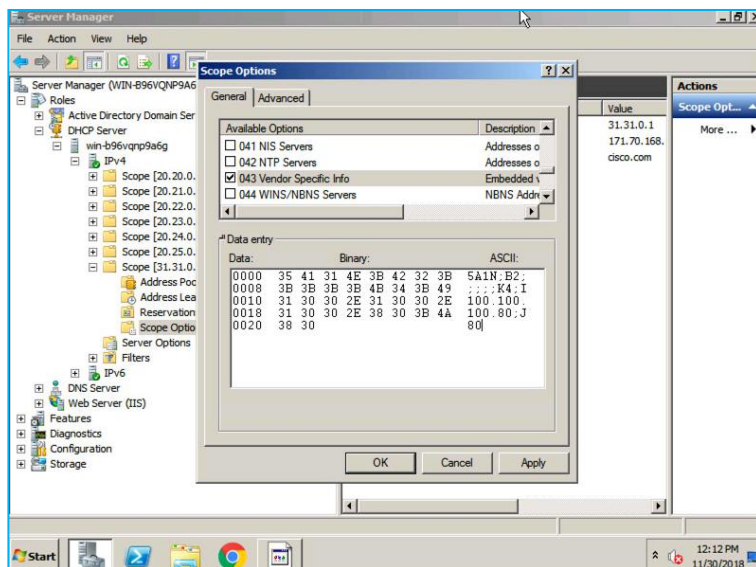
When the sensor receives its own IP address from the DHCP server, it also gets the Cisco DNA Center IP address through the DHCP Option 43 field.

Sample configuration from Cisco IOS device:

```
ip dhcp pool vlan30
 network 30.30.0.0 255.255.0.0
 default-router 30.30.0.1
 dns-server 100.100.100.11
 option 43 ascii 5A1N;B2;K4;I100.100.100.80;J80
```

Sample configuration (screen shots) from Windows server:

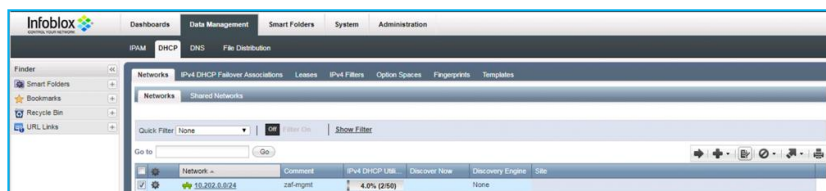
Option 43 Configuration on Windows Server



Use uppercase letters to configure the Option 43 field.

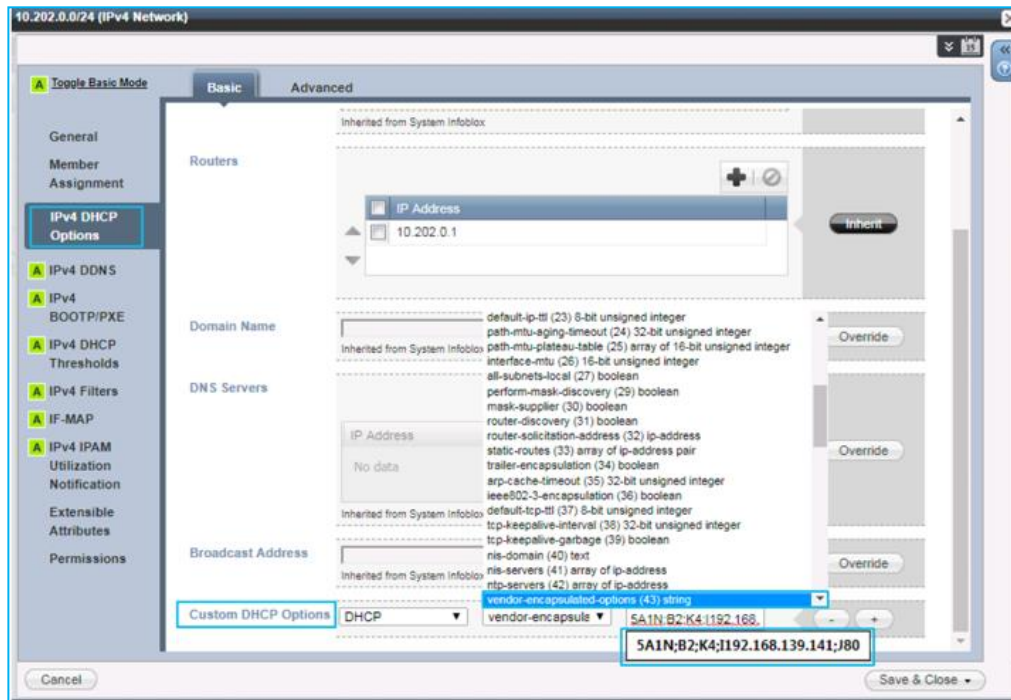
For Infoblox, under **Data Management > DHCP > Networks**, choose the IPv4 network and click **Edit**.

Step 1: Option 43 Configuration on Infoblox

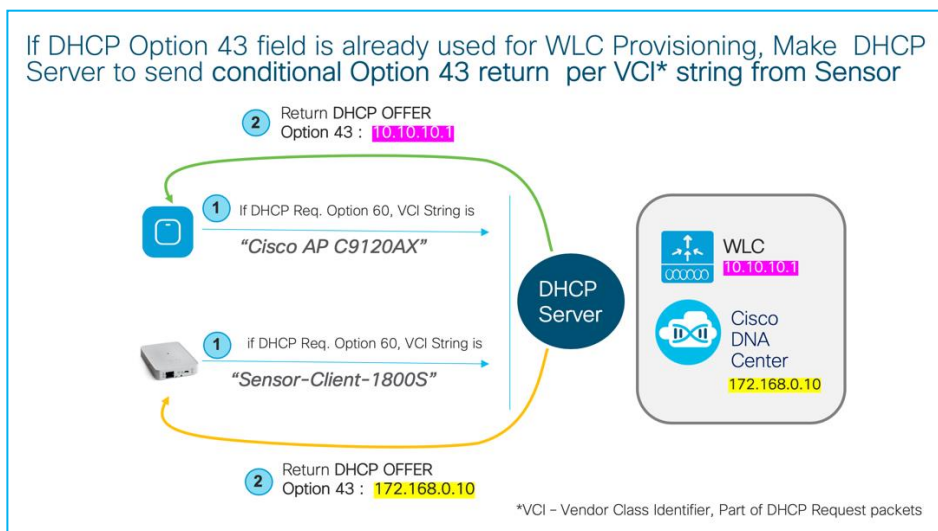


1. Choose IPv4 DHCP options.
2. Under the Custom DHCP options area, choose DHCP and vendor-encapsulated-options (43) string. Enter the Option 43 ASCII string, such as 5A1N;B2;K4;192.168.139.141;J80.

Step 2: Option 43 Configuration on Infoblox



If the DHCP Option 43 field is already used for another purpose (such as to send the wireless controller IP address to the AP), you can configure the DHCP server to return a different Option 43 message based on the client device type. To identify the client device type, validate the identifier message (DHCP Option 60) within the DHCP request packet from the client (in this case, the Cisco 1800S Sensor).



When the sensor sends the DHCP request, it always includes the DHCP Option 60 field, Vendor Class Identifier (VCI). The VCI is a text string that uniquely identifies the vendor of the DHCP client device. The Cisco 1800S sensor VCI string is *Sensor-Client-1800S*.

To use the special VCI string, the DHCP server administrator must make a special conditional handling of the Option 43 return field. Based on the incoming VCI string, the DHCP server can return different IP addresses.

For example, if the DHCP client includes VCI string *Cisco AP c3800*, it means the DHCP client is a regular Cisco AP 3800 and needs to get the Cisco wireless controller's IP address as part of the Option 43 message. If the DHCP request message includes the VCI string *Sensor-Client-1800S*, it means the client device is a Cisco 1800S Sensor, and the Option 43 field from the DHCP server is the Cisco DNA Center IP address.

You can find different VCI string examples at <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html>.

In addition to Option 43, if the sensor has an 8.7.258 image, the sensor requires the NTP server IP address. The DHCP server includes the NTP server IP address in the Option 60 field. This information is not required if the sensor software is 8.8.261 or later, because the NTP server information is transferred as part of the sensor PnP provisioning process.

For information about DHCP options for PnP, see <https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/97066-dhcp-option-43-00.html>.

DNS-Based Cisco DNA Center Discovery

You can create a host record on the DNS server for the domain with the name *PNPSEVER* and the IP address of Cisco DNA Center. The sensor uses the DHCP received domain name to create the fully qualified domain name (FQDN) and make a *pnpserver.domainname.com* query to the DNS server for the Cisco DNA Center IP address. If Cisco DNA Center has a custom or CA signed certificate, the certificate must contain the PNP FQDN string in the SAN DNS entries. Make sure Cisco DNA Center has domain name configured because if Cisco DNA Center installed without domain name, DNS-based Discovery will be failed.

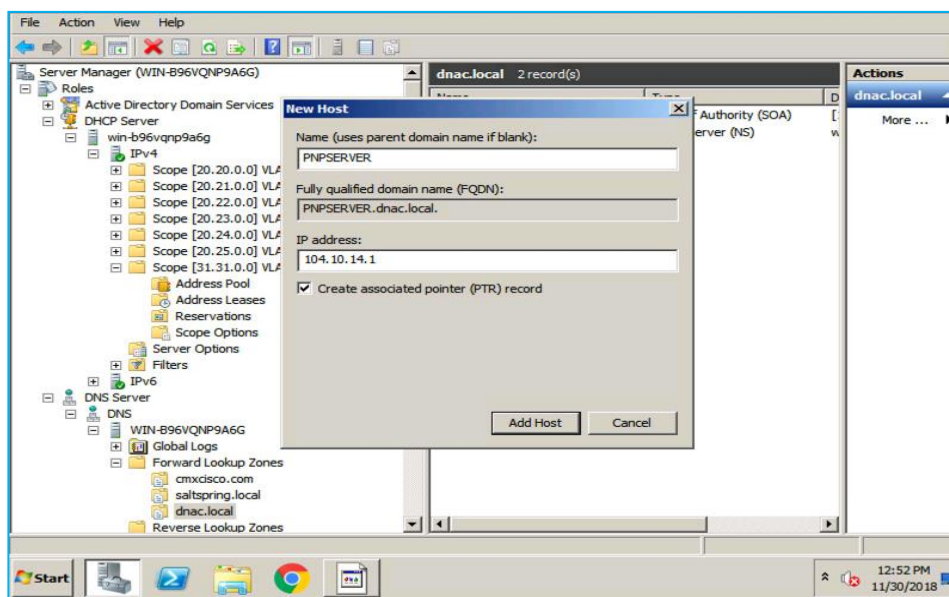
For more information on DNS name-based discovery, see https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#con_115728.

Note: Make sure the IP DHCP pool has the dns-server (Option 6) and the domain name (Option 15) configuration.

Example:

```
ip dhcp pool vlan30
network 30.30.0.0 255.255.0.0
default-router 30.30.0.1
domain-name Cisco DNA Center.local
dns-server 100.100.100.11
```

DNS Configuration - Windows Server



Cisco DNA Provisioning Through CLI

Starting with Cisco 1800S Sensor Release 8.8.257.0, you can configure Cisco DNA Center manually through the sensor CLI.

Connect the sensor through the special console cable (AIR-CONSADPT=).

Log in to the sensor with the default username and password (Cisco/Cisco). Enter privileged mode with prompt (#) and then enter the following command line:

```
#config dot11 sensor pnp ip <ip address of Cisco DNA Center>
```

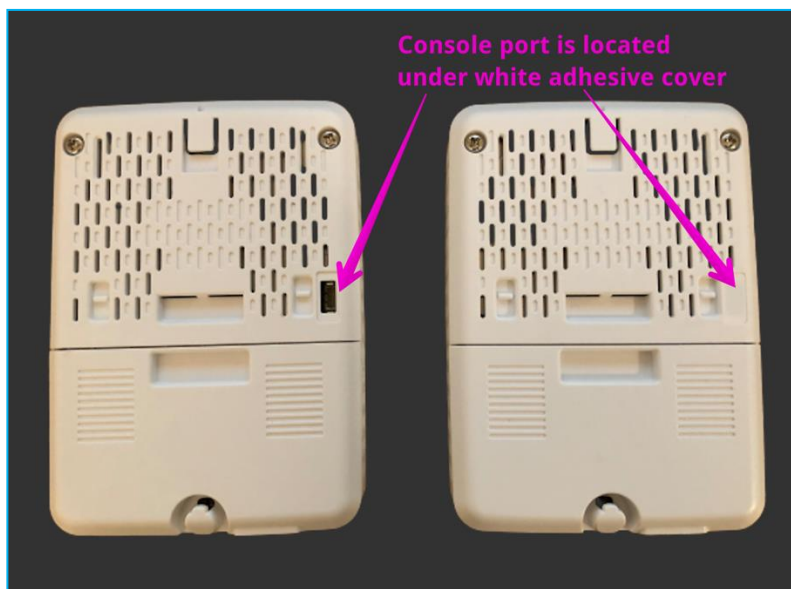
Example:

```
#config dot11 sensor pnp ip 100.100.100.80
```



If the sensor is running Cisco 1800S Sensor Release 1.3.3 or later, day-0 SSH is available. Day-0 SSH offers remote SSH access to sensors, but it doesn't allow privileged mode access.

One caveat is the location of sensor's console port, which is located under the white adhesive cover.



To provision Cisco DNA Center manually using remote access, enter:

```
> config dot11 sensor pnp ip <Cisco_DNA_Center_IP_address>
```

This feature is useful when the sensor is deployed onsite without staging, or when it is reset to the factory default. The network administrator can find the sensor's IP address by using the CDP neighbor details, and SSH into the sensor and Cisco DNA Center IP address.

Similarly, to configure the NTP IP address, enter:

```
#configure dot11 sensor ntp ip <NTP_server_ip_address>
```

Note: Typically, you don't need to configure NTP, because the NTP IP address can be provided as part of the provisioning process with the 8.8.261 image.

Connect Your Sensor to the Network

The sensor requires one logical interface, the special purpose *backhaul interface*, which provides network connectivity between the sensor and Cisco DNA Center.

The sensor can use *wired* (using the PoE module) or *wireless* backhaul. For wireless backhaul, the admin must choose one SSID from the existing WLAN setup. Keep in mind that backhaul SSID creation is not a part of Cisco DNA Center automation. The admin can choose any SSID that is created by Cisco DNA Center or manually created from the wireless controller.

The sensor uses backhaul to:

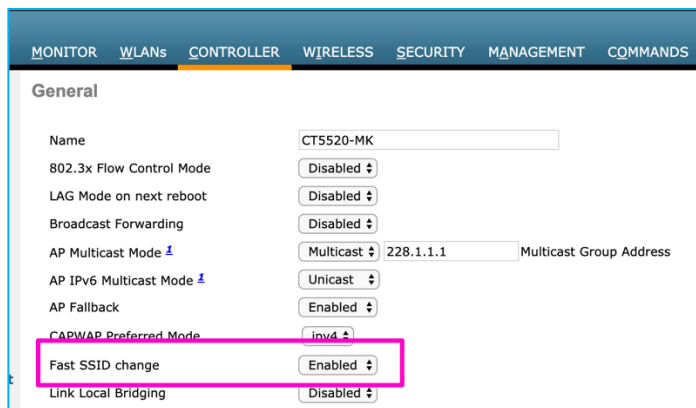
1. Enable the keepalive heartbeat exchange between Cisco DNA Center and the sensor (HTTPS, heartbeat every minute).
2. Download the new sensor test configuration.
3. Upload the sensor test result.
4. Upgrade the sensor image.

The preceding sensor operations use HTTPS.

When the sensor uses wireless backhaul, the sensor switches frequently between the test target SSID and the wireless backhaul SSID. For example, when the sensor finishes a series of tests from the configured AP in the 2.4-GHz band, the sensor switches the SSID to the backhaul SSID and reports results to Cisco DNA Center.

After reporting is finished, the sensor reconnects to the test SSID and runs testing on the other band. Similarly, the sensor comes back regularly to Cisco DNA Center for a heartbeat. Ultimately, the sensor cycles through test SSID1 > backhaul SSID > test SSID2 > backhaul SSID > test SSID3 and time slices wireless testing, reporting, and heart beating.

Because of this unique behavior, we recommend that you enable **Fast SSID change** from the wireless settings. The **Fast SSID change** does not impact sensor test results or sensor operation.

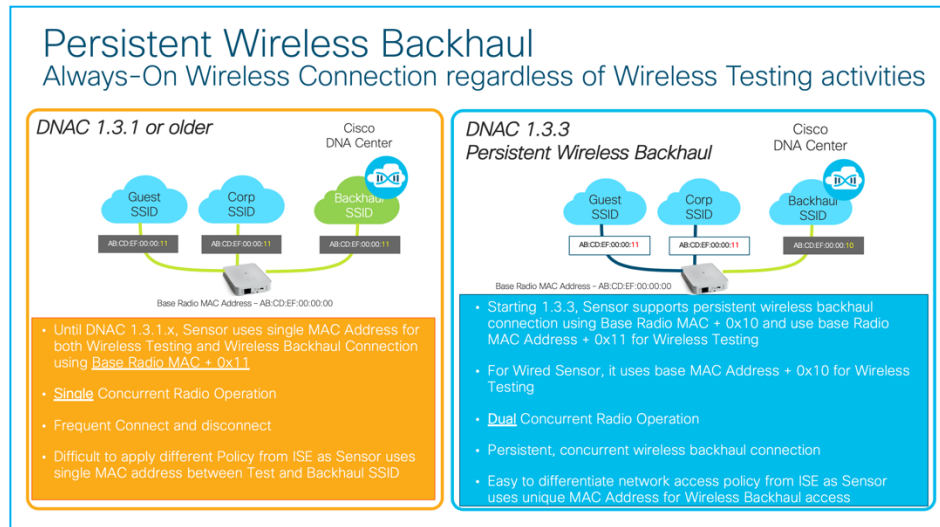


For the Cisco Catalyst 9800 switch, **Fast SSID change** is enabled by default.

Persistent Wireless Backhaul

If the sensor is running 1.3.3 or later, it supports *persistent wireless backhaul*, which is a dedicated wireless connection from the sensor to Cisco DNA Center. As long as the sensor test band remains in single band, persistent wireless backhaul is maintained. When the wireless

test band changes, the wireless backhaul connection shifts to the other band. The sensor uses the virtual MAC address (radio MAC address + 0x10) to maintain the persistent wireless backhaul connection to the AP.

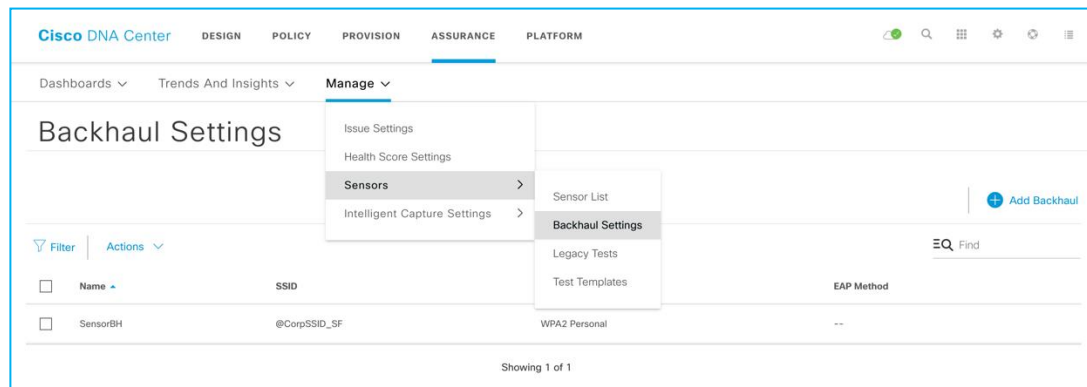


Create a Sensor Backhaul Profile in Cisco DNA Center

A Cisco sensor backhaul profile is essential to claim the sensor from the PnP page. The PnP Claim page has a default sensor backhaul profile named *CiscoSensorProvisioning*.

Because of the default *CiscoSensorProvisioning* profile, you don't need to create a custom sensor backhaul profile unless you want to use an SSID other than *CiscoSensorProvisioning* for the wireless backhaul SSID.

To create a new sensor backhaul configuration, log in to Cisco DNA Center and choose **Assurance > Manage > Sensors > Backhaul Settings**. Click **Add Backhaul**. (The setting is local to Cisco DNA Center and is not pushed to the wireless controller.)



Ensure that the SSID name matches an existing WLAN. Also, ensure that the security matches.

The following WLAN security is supported:

- WPA2-Enterprise (PEAP-MSCHAPv2, EAP-FAST)
- WPA2-PSK
- Open

We recommend that you use the latest Cisco 1800S Sensor Release 1.3.3.0 for wireless backhaul operation.

Sensor Backhaul Settings from Cisco DNA Center

If the sensor is assigned an SSID that is different from the *CiscoSensorProvisioning* SSID, the sensor does not use the *CiscoSensorProvisioning* SSID after PnP provisioning, because it's configured with a new backhaul SSID. If the backhaul SSID fails to connect, the sensor falls back to the *CiscoSensorProvisioning* SSID.

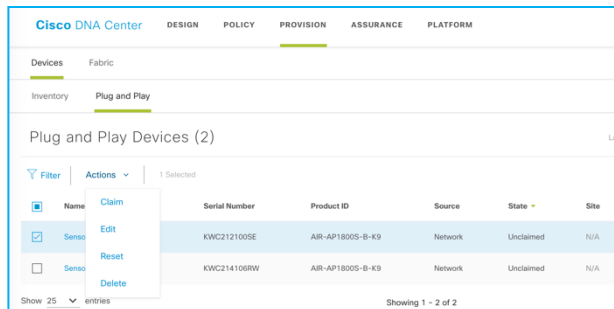
Provision the Sensor: Claim the Device

The following steps explain how to claim the sensor.

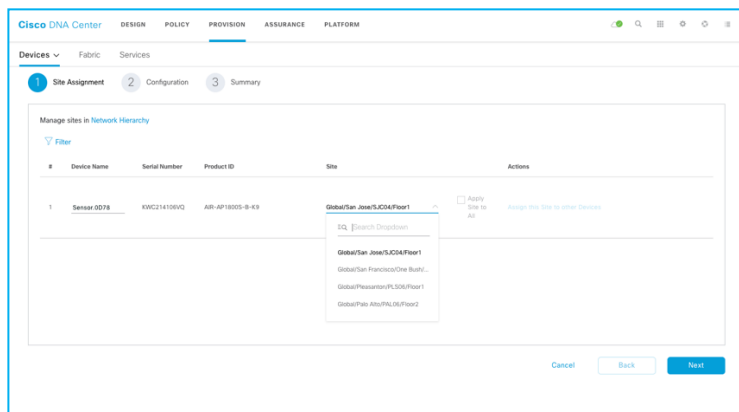
1. If your sensor has a PoE module, connect your sensor to the PoE port on the switch.
2. If your sensor uses a wireless backhaul connection, power the sensor by plugging it into a wall power socket or use the adapter and attached micro USB-B connector. For either backhaul type, ensure that the sensor has HTTP (TCP 80) and HTTPS (TCP 443) reachability to the Cisco DNA Center server.
3. After the sensor is powered on, wait for approximately 5 minutes. If the sensor has reachability to the Cisco DNA Center server, the sensor appears in an unclaimed state under **Provision > Devices > Plug and Play**.
4. Before claiming the sensor, you can change the default sensor name to the desired name.

In Cisco DNA Center Release 1.3 or earlier, you can change the sensor name only at this stage. After you claim the sensor, you cannot change the sensor name unless you delete it from the inventory.

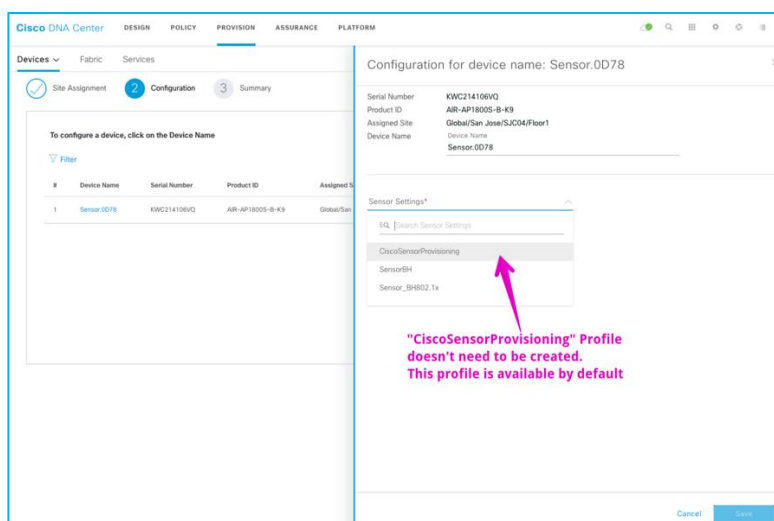
To change the sensor name, go to **Provision > Devices > Plug and Play**. Select the target sensor and choose **Actions > Edit**.



- After you change the sensor name, your sensor is ready to be provisioned. Select the sensor from the **Unclaimed Device** list and click **Claim Device**.



The first step of the claim process is picking up the sensor deployment location.



6. If you didn't create a sensor PnP profile, you can use the default CiscoSensorProvisioning sensor profile. If you are deploying a wired sensor, you must still choose one profile, in which case the default profile is a convenient option.

Note: If you want to change the sensor name after the PnP claim, go to **Assurance > Manage > Sensor > Sensor List > Edit Sensor Name(s)**.

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes DESIGN, POLICY, PROVISION, ASSURANCE, and PLATFORM. The 'Manage' tab is selected under the 'Sensor List' section. A table lists sensors with columns for Name, Location, and Backhaul Type. A context menu is open over the first three rows, with 'Edit Sensor Name(s)' selected. A side panel titled 'Edit Sensor Name(s)' is open on the right, showing fields for Name, Suffix, and a list of selected sensor serial numbers.

Cisco 1800S Sensor Provisioning – Claiming Device

The screenshot shows the Cisco DNA Center interface. The top navigation bar includes DESIGN, POLICY, PROVISION, ASSURANCE, and PLATFORM. The 'Devices' tab is selected under the 'Plug and Play Devices' section. A table lists devices with columns for Serial Number, Product ID, Source, State, Site, and Last Contact. The 'Claim' button is highlighted with a red arrow. The 'State' column is circled in red, showing 'Unclaimed' for the first three devices.

The device status changes from **Unclaimed > Planned > Onboarding > Provisioned**. The device remains in the provisioned state, unless it fails to be provisioned. In this case, the sensor changes to an error state. Any errored entries remain even if the device is removed from the network.

Cisco 1800S Sensor Provisioning – Workflow

The screenshot displays the Cisco DNA Center interface. On the left, under 'Devices', there is a table titled 'Plug and Play Devices (5)' with columns for #, Device Name, Serial Number, Product ID, and Status. Five sensors are listed, all with a status of 'Not'. The right pane shows the details for sensor KWC21130004, which is 'SUDI: Authenticated'. It includes tabs for Details, History, and Configuration. The History tab is active, showing a list of events with columns for Status, Time, Details, and Info. The events include tasks like 'Site Config Task Completed', 'Site Config Task', 'Config Generated', 'Config Requested', 'User Workflow', 'Device Claimed', 'Device Authenticated', and 'Device Secured'.

When the sensor is in Managed state, it's ready to download the sensor-driven test config and run the sensor test.

If the sensor changes to an error status, you can view the error details under the **History** tab. You can always delete a sensor with an error status; that sensor returns to the list in an unclaimed state.

Upgrade the Sensor Software in 8 Steps

8 Step Sensor Image Upgrade through Cisco DNA Center

Prep – Image Management

- 1 Tag New sensor image as Golden Image ★
- 2 Click [Update Device] [Update Devices](#)

Upgrade

- 3 Select Upgrade Target Sensor
- 4 Action > Update OS Image
- 5 [Distribute] select "Now"
- 6 [OS Update] Select "Schedule Activation after Distribution is completed"
- 7 "Confirm" Upgrade
- 8 Wait for SWIM to complete upgrade

... or using CLI via Console or SSH

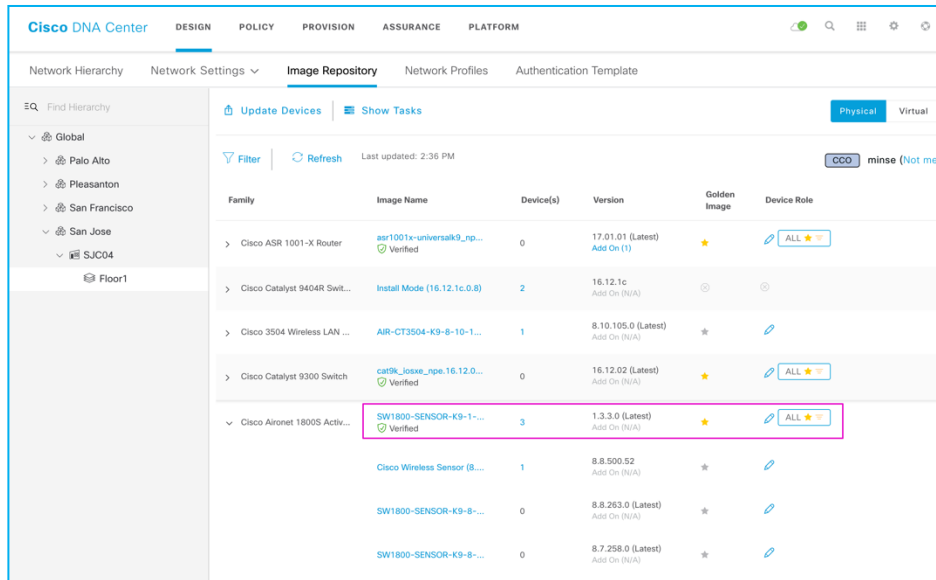
```
# archive download-sw /reload tftp://192.168.0.1/SW1800-SENSOR-K9-1-3-3-0.tar.gz
```

After you provision the sensor, you can update the sensor software to the latest release. Currently, the Cisco 1800S Sensor Release 1.3.3.0 is the latest, and it aligns with the latest Cisco DNA Center Release 1.3.3.0. After you enter your CCO ID and password into Cisco DNA Center, Cisco DNA Center Assurance automatically retrieves the list of device images from Cisco.com.

You need to first mark the new image as a golden image so that it is used as the new sensor software.

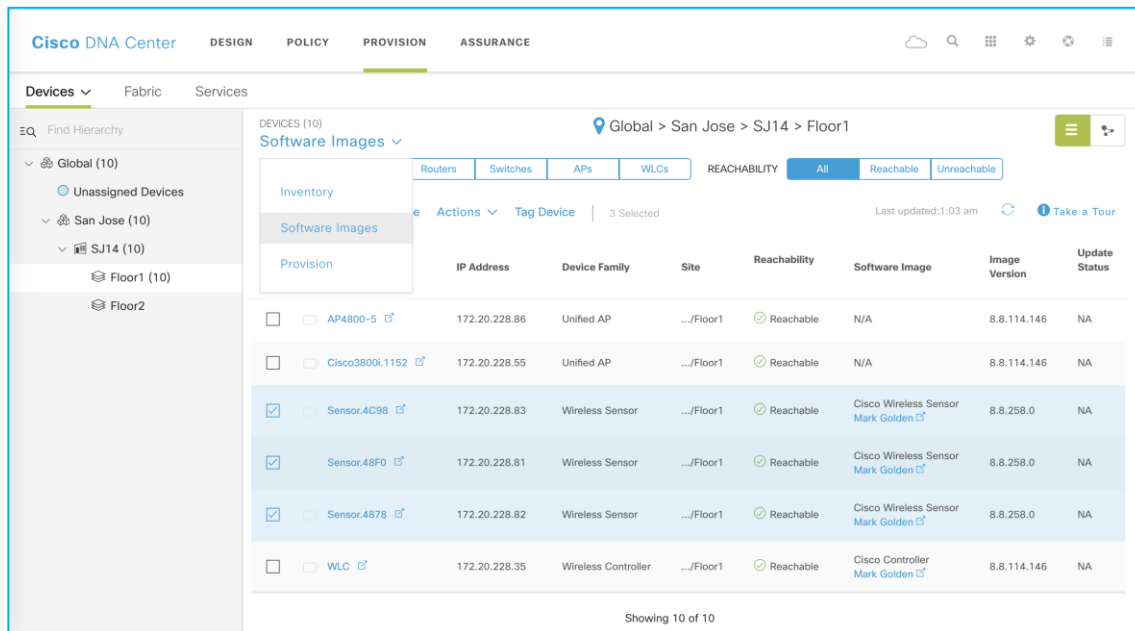
You mark the new sensor software as the golden image by clicking the Star icon next to the desired image in the list. Cisco DNA Center starts to retrieve the new software from Cisco.com.

Alternatively, you can manually import the sensor software into Cisco DNA Center from your local browser. Import the sensor software from the Image Repository tool, which is integrated as part of Design option in Cisco DNA Center 1.3, by clicking **Design > Image Repository**.



After preparing the golden image, you can start the image upgrade from the Inventory page. The first step is to select the target sensors to be upgraded.

After you select all the sensors, click **Action** and select **Image Upgrade**. Make sure all selected sensors are in manage status.



1. Click **Now** and then **Next**. (Alternatively, click **Later** to schedule the upgrade for a later time.)
2. Check the **Schedule Activation after Distribution is completed** check box.

3. Click **Confirm** to initiate the image upgrade.

There are couple of conditions where the sensor image upgrade can fail. For example:

- The golden image has not been selected. After you confirm the upgrade target image on the Image Repository page, you need to manually click the Star icon next to the image version. This selection determines the upgrade target image.

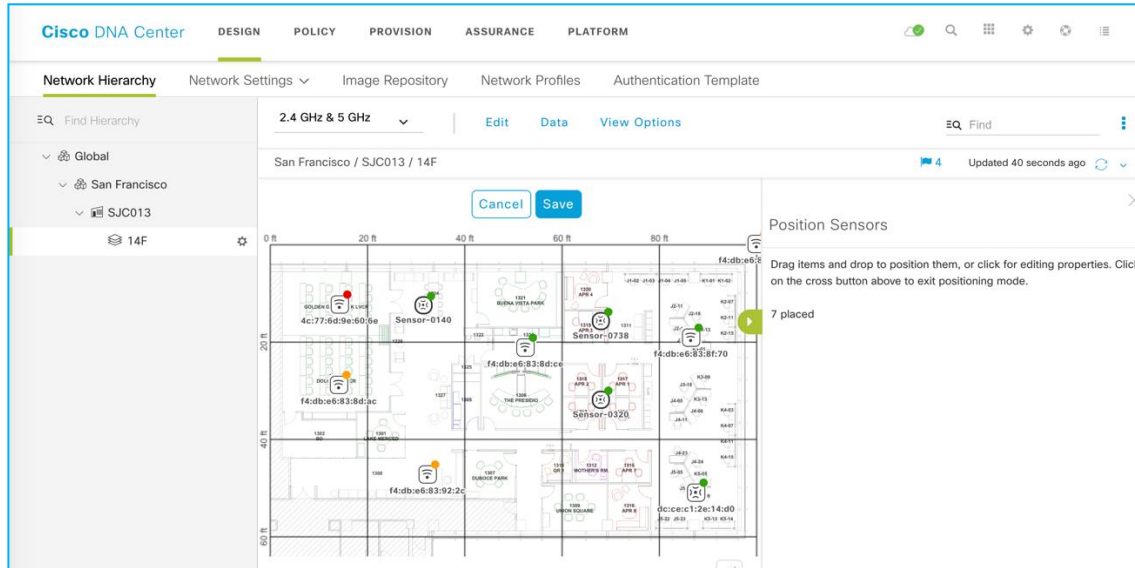


- The sensor is in a partial collection failure status. This status means that the sensor failed to exchange heartbeats with Cisco DNA Center. In this case, the image upgrade is not initiated. Only after all of the selected sensors are ready to be upgraded can select **Now** to start the upgrade of all selected sensors.
- When multiple sensors are selected as upgrade targets and any of the selected sensors experiences the conditions in the above bullets, the image upgrade is not initiated.

Place the Sensor on the Floor Map

You can also provision sensors from the floor map in the Design section.

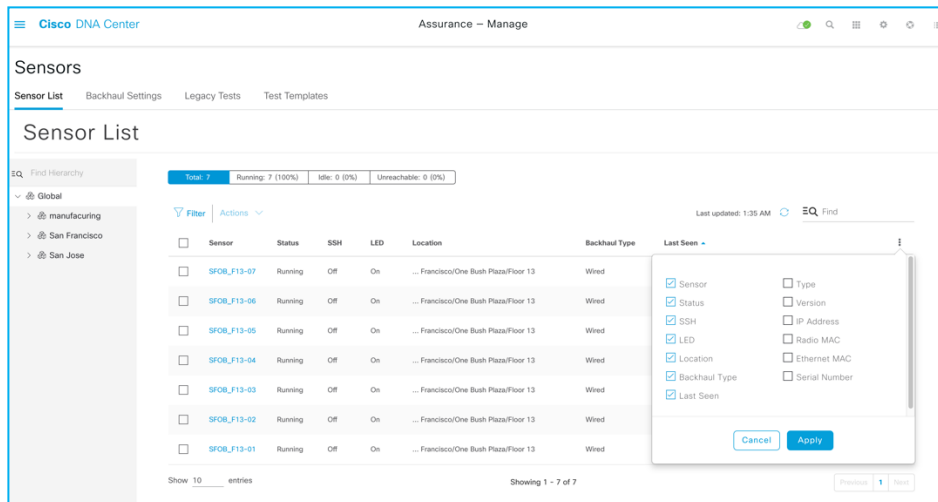
Choose **Design > Network Hierarchy > (Desired Floor)** and click **Edit**.



You can drag and drop sensors from the upper right corner of the map to the current placement of sensors and click **Save** to apply the changes to the map. The floor map shown above is displayed during sensor selection step.

Manage Sensors

Sensor List page



The **Sensor List** page was added in Cisco DNA Center Release 1.3.1. This page allows you to change various sensor settings such as **Sensor Name**, **SSH Username** and **Password**, **LED**, and **Backhaul Type**.

Note: A sensor uses a single admin ID between SSH and CLI, so if you change the username and password of a sensor, both the SSH and CLI login credential are changed.

The default sensor username and password are Cisco/Cisco. When you configure a username and password, this default value is overwritten.

Also, from the Sensor List page, you can check a sensor's current operational status (**Running**, **Idle**, or **Unreachable**) and many other attributes.

Create a Sensor Test Template

To create a test suite, choose **Assurance > Manage > Sensors > Test Templates** and click **Add Sensor Test**.

Test Name	SSID with Test Types	AP Coverage	Location	Schedule
demo	SJC_SSID: Onboarding, RF Assessment	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Deploy Test	N/A
MySensor123	@CorpSSID: Onboarding, RF Assessment @CorpSSID_PSK: Onboarding, RF Assessment	5GHz: 1, -70dBm	Global/manufacturing	Continuous Run Now
SensorTest	@CorpSSID: Onboarding, RF Assessment, Net.Service, App.Connectivity, Performance @CorpSSID_PSK: Onboarding, RF Assessment, Net.Service, App.Connectivity, Performance	2.4GHz: 2, -70dBm 5GHz: 3, -70dBm	Global/San Francisco	Continuous Run Now
T13	SJC_SSID: Onboarding, RF Assessment	2.4GHz: 1, -73dBm	Deploy Test	N/A
test	SJC_SSID: Onboarding, RF Assessment, Net.Service	2.4GHz: 3, -70dBm 5GHz: 1, -70dBm	Deploy Test	N/A

Showing 5 of 5

The new sensor test templates provide many advantages compared to the legacy sensor test suite.

- The template can be assigned to multiple floors and sites. You don't need to repeatedly create a sensor test for every floor.
- The template allows unique sensor test configuration per SSID. Previously, all configured SSIDs shared the same test configuration.
- The sensor coverage threshold is configurable per band.
- The new RF assessment test uses RF parameters collected from other testing.
- The **Run Now** option has been added.
- The sensor test interval was expanded from 7 minutes to 24 hours.
- The sensor test can be enabled by time of day and day of week.
- A new sensor test interval called **Continuous** has been added. This interval allows the sensor to run continuously without stopping.
- A single sensor can use only the single sensor test template, so you know exactly what test is running per sensor or per location.
- Certain sensor tests can take a long time, and total sensor test duration is varied based on number of selected sensor test types. Minimum sensor test interval is automatically adjusted based on estimated sensor test duration.
- Support of an HTTPS test has been added.

- You configure templates using a new UI workflow.
- Sensor test can be easily duplicated, edited, deployed, and undeployed.

Cisco DNA Center performs the following network service and application tests:

- **Wireless Onboard Test:** Cisco DNA Center connects to an SSID with credentials and gets the IP address through DHCP. It then verifies the gateway and DNS server received through DHCP.
- **RF Assessment Test:** Cisco DNA Center collects various RF performance measurements, such as transmit and receive data rates and SNR (Signal-To-Noise Ratio) during the active sensor testing and assesses the quality of the RF environment.
- **DNS Test:** Cisco DNA Center resolves IP addresses from the domain name.
- **Host Reachability Test:** Cisco DNA Center verifies reachability using the Internet Control Message Protocol (ICMP) echo request.
- **RADIUS Test:** The sensor acts as a RADIUS authenticator and authenticates through a wireless device. The sensor can test the RADIUS server using the Password Authentication Protocol (PAP) or the Microsoft version of the Challenge-Handshake Authentication Protocol (MS-CHAP).

Note: If you have a Wi-Fi onboarding test that includes 802.1x/EAP authentication, then this RADIUS test is already covered as part of the onboarding test.

Cisco DNA Center supports the following performance tests:

- **Speed Test:** Cisco DNA Center performs tests against the Network Diagnostic Tool (NDT) servers in the internet to obtain the downlink and uplink throughput and latency. Here is test sequence:
 - a. The sensor sends an HTTP query to the M-Lab server to get the nearest M-Lab server information.
 - b. The sensor uses the returned NDT server cluster information.
 - c. The sensor accesses the NDT server using TCP port 3001.
- **IP SLA Test:** The sensor sends a UDP probe to the AP that functions as a responder to determine the jitter, latency, packet loss and round-trip time of the last hop.

Note: The network infrastructure must be running software release 8.8.111 or later to perform these tests.

For IP SLA, the sensor connected to the AP which has the IP SLA responder feature. IP-SLA Responder feature is available on Wave 2 APs - AP1800, AP2800, AP3800 and AP4800 series and 802.11ax APs – Catalyst 9100 series AP with AireOS 8.8 or above or IOS-XE 16.12.1s or above software.

Cisco DNA Center supports the following application tests:

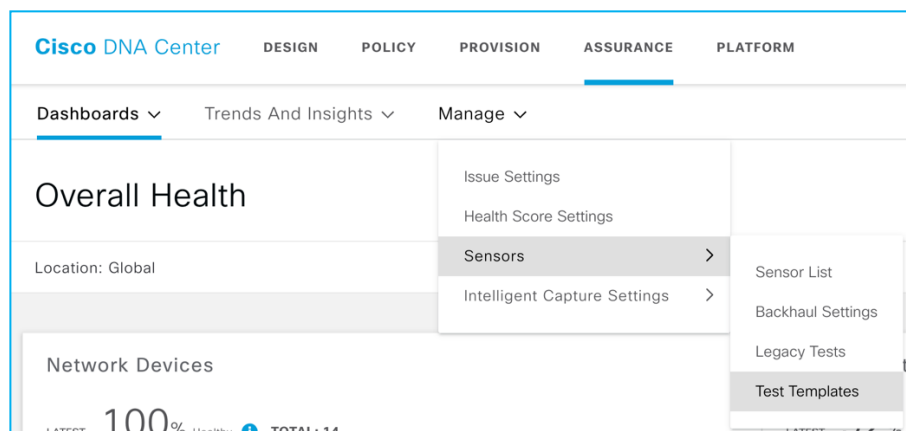
- **Email:**
 - **Internet Message Access Protocol (IMAP):** Cisco DNA Center connects to an IMAP server TCP port (143).
 - **Post Office Protocol3 (POP3):** Cisco DNA Center connects to a POP3 server TCP port (110).
 - **Outlook Web Server (OWS):** Cisco DNA Center logs into the OWS (with On-Premise Exchange Server) and verifies access.
- **File Transfer:** Cisco DNA Center tests for upload or download file operation using FTP protocol.
- **Web (http, https):** Cisco DNA Center tests for access to the provided URL and verifies the response data.

Procedure

Create a Sensor Test Template

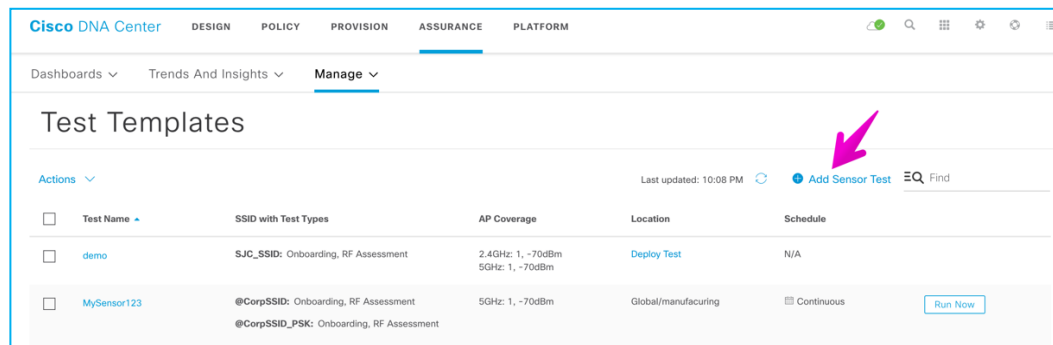
1. To create the test suite, choose **Assurance > Manage > Sensors > Test Templates**.

Sensor Tests Templates - Navigation



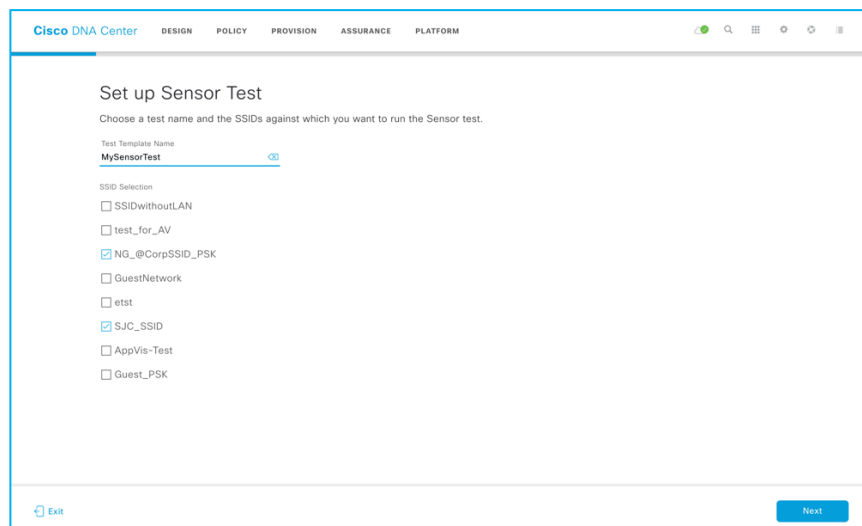
2. Click **Add Sensor Test**.

Add Sensor Test



3. From the **Set up Sensor Test** page, enter a template name and choose an SSID.

Set Up Sensor Test



4. After you choose the test target SSID, enter the credentials for sensor wireless onboarding.

The screenshot shows the 'Enter SSID Credentials' page in Cisco DNA Center. The page title is 'Enter SSID Credentials' with a subtitle 'Specify the SSID details necessary to run the Sensor test.' There are two expandable sections. The first section is for SSID: NG_@CorpSSID_PSK, showing Security: WPA2 Personal and a Password field with a 'SHOW' link. The second section is for SSID: SJC_SSID, showing Security: WPA2 Enterprise, EAP Method: PEAP-MSCHAPv2 (with a dropdown arrow), User Name: Sensor, and a Password field with a 'SHOW' link. At the bottom, there is an 'Exit' button and 'Previous' and 'Next' buttons.

5. If the selected SSID has WPA2 Enterprise security type, choose EAP (Extensible Authentication Protocol) type. The three types of EAP protocol supported are **EAP-FAST**, **PEAP-MSCHAPv2**, and **EAP-TLS**.
6. If you select the EAP-TLS method, you need to select and upload a certificate (PKCS#12 bundle, *.pfx). Then, enter the password associated with the certificate bundle to decrypt it. You also need to supply a username.

EAP-TLS

EAP-TLS certificates must be in *.pk12 or *.pfx format. The certificate bundle should include 1) user certificate 2) root CA and 3) certificate bundle password. Both extensions qualify as a PKCS #12 archive file format. This is the only type of file format that the sensor accepts.

The following example shows how to generate and EAP-TLS certificate with ISE:

Note: Refer to the following document to setup the certificate provisioning portal in ISE and to generate certificates:

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200534-ISE-2-0-Certificate-Provisioning-Portal.html>

- From the ISE **Certificate Provisioning Portal**, enter the fields as highlighted in the screen shot below.
- Click generate to generate the certificate. This will generate a .zip file and download it to your laptop.
- Unzip the file to obtain the certificate in pk12 format. Use this certificate when scheduling a test suite that uses EAP-TLS as the EAP method.

ISE EAP TLS Certificate generation

The screenshot shows the Cisco Certificate Provisioning Portal interface. The form is titled 'Certificate Provisioning' and includes the following fields and annotations:

- I want to:** A dropdown menu with the option 'Generate a single certificate (without a certificat...)' selected.
- Common Name (CN): *** A text input field containing 'sensortis'. A red arrow points to this field with the annotation '(Enter identity as found in "Identities")'.
- MAC Address: *** A text input field containing '70-43-5a-7f-8a-e0'. A red arrow points to this field with the annotation 'MAC Address of Sensor from Inventory Page of DNA'.
- Choose Certificate Template: *** A dropdown menu with the option 'TLSCert' selected.
- Description:** A text input field containing 'TLS Cert for Sensors'.
- Certificate Download Format: *** A dropdown menu with the option 'PKCS12 format, including certificate chain (...)' selected. A red arrow points to this field with the annotation 'PKCS12 format including certificate chain and password'.
- Certificate Password: *** A password input field with a masked password '*****'.
- Confirm Password: *** A password input field with a masked password '*****'.
- Buttons:** 'Generate' and 'Reset' buttons at the bottom of the form.
- Help:** A link at the bottom of the form.

WebAuth Enabled SSIDs

Provide the following for Layer 3 security, if WebAuth is enabled on the SSID:

- For WebAuth with user authentication, provide the necessary credentials.
- For WebAuth with Passthrough, you can choose to provide an email address.

Note: Only Internal WebAuth (that is, web authentication performed by the WLC) is supported with the sensor.

7. Click **Next** to go to the **Select Tests** page.

Add Sensor Tests - Network Tests

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Define Sensor Test Category Details

Specify the Sensor Test Category Details to see results for

- > SSID: NG_@CorpSSID_PSK
- SSID: SJC_SSID
 - Onboarding
 - ☒ Association
 - ☒ Authentication
 - ☒ DHCP
 - RF Assessment
 - ☒ Data Rate
 - ☒ SNR
 - Network Services Tests
 - ☐ DNS
 - ☐ RADIUS

[Exit](#) [Previous](#) [Next](#)

Performance Tests – Speed Test

Performance Tests

☒ Speed Test

NDT Server (optional) Proxy Server (optional)

MLAB Map Satellite

Speed tests use distributed NDT (Network Diagnostic Tool) from the “mlab” server in the cloud.

If you leave the **NDT Server** IP address field empty, the sensor sends an HTTP query to the “mlab” server (<http://mlab-ns.appspot.com/ndt?format=json>) to get the nearest “mlab” server information, as follows:

```
{ "city": "San Francisco Bay Area_CA", "url": "http://ndt.iupui.mlab2.nuq07.measurement-lab.org:7123", "ip": ["209.170.110.216", "2001:2030:0:12::216"], "fqdn": "ndt.iupui.mlab2.nuq07.measurement-lab.org", "site": "nuq07", "country": "US" }
```

Now the sensor uses the returned NDT server cluster information to run actual performance testing. The sensor uses TCP Port 3001 for performance testing.

The M-Lab server provides the NDT server information so you don’t need to prepare the server. Typically, the private NDT server is not available, so the **NDT Server** IP address field remains blank.

If the connection to the internet requires a proxy server, you can add one. The proxy server address needs to be an IPv4 address, because FQDN format is not yet supported

Performance Tests – IP SLA

Performance Tests

☐ Internet (NDT)

☒ IP SLA

Gold

- Platinum
- Gold**
- Silver
- Bronze

In IP Service Level Agreement (SLA) testing, the sensor measures IP SLA performance using a UDP Echo/Jitter probe against a connected AP. When the sensor sends IP SLA traffic, the AP terminates the IP SLA traffic at the first hop, regardless of whether or not the AP is in traffic forwarding mode (local, Flex, or Fabric). IP SLA traffic can choose different Wi-Fi Multimedia (WMM) up tagging value to simulate wireless performance in various QoS conditions.

IP SLA testing is supported on Wave-2 (AP1800/2800/3800/4800 series AP) and Wi-Fi 6 APs (Catalyst 9100 series) models running software release 8.8.111 or 16.12.1s.

IP SLA UDP Probe Packet QoS Marking

Service Level	WMM UP	DSCP
Platinum	6	46 (EF)
Gold	5	34 (AF41)
Silver	2	18 (AF21)
Bronze	1	10 (AF11)

Test target SSID QoS level should be higher than sensor IP SLA configured QoS value. For example, if the SSID QoS setting is Gold, and the sensor IP SLA QoS setting is Platinum, the AP cannot prioritize Platinum.

Add Sensor Tests - Application Tests

Application Tests

☐ Host Reachability

☒ Web

URL*

www.cisco.com

URL*

http or https... × ⊕ Add

☐ FTP

Create a Sensor Test Template

The application test measures serviceability and time to connect.

Note: Outlook Web Access supports only Exchange Server and not Office 365. Web Test supports HTTP and HTTPS. You can use a FQDN as the URL.

Add Sensor Tests - File Transfer Tests

File Transfer Tests

☒ FTP

Server IP: 100.100.100.100 User Name: ftpuser

Password: Protocol: ftp

Transfer Type: **UPLOAD** Download File Path/Upload Path: /home/ftuser
(Provide only the path for Upload)

Server IP: 100.100.100.100 User Name: ftpuser

Password: Protocol: ftp

Transfer Type: **DOWNLOAD** Download File Path/Upload Path: /home/ftuser/dnac-test

Note: The name of the internal file that gets uploaded in an upload test is "FTP_UPLOAD_FILE_[Sensor MAC Address].txt" When you choose **Download** or **Upload** or **Download**, choose a file that is smaller than 5 MB.

8. Click **Next** to go to the **Select AP Coverage** page.

Cisco DNA Center DESIGN POLICY PROVISION ASSURANCE PLATFORM

Select AP Coverage

Choose the Coverage Target against which to run the Sensor test.

Band
☒ 2.4GHz

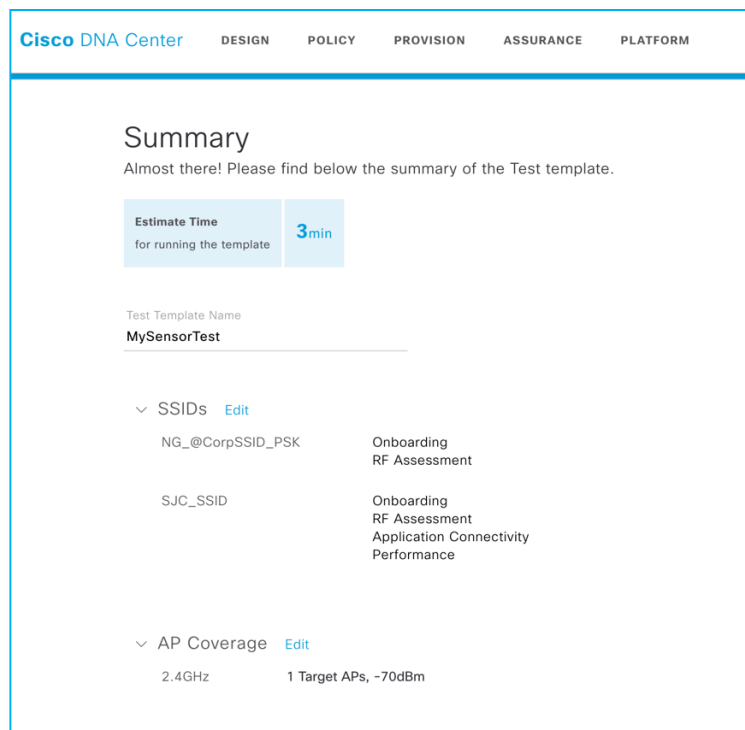
Test Coverage Per Sensor
Number of Target APs: 1
RSSI Range: -90 to -35 dBm (set at -70 dBm)

Band
☐ 5GHz

Test Coverage Per Sensor
Number of Target APs: 1
RSSI Range: -90 to -35 dBm (set at -70 dBm)

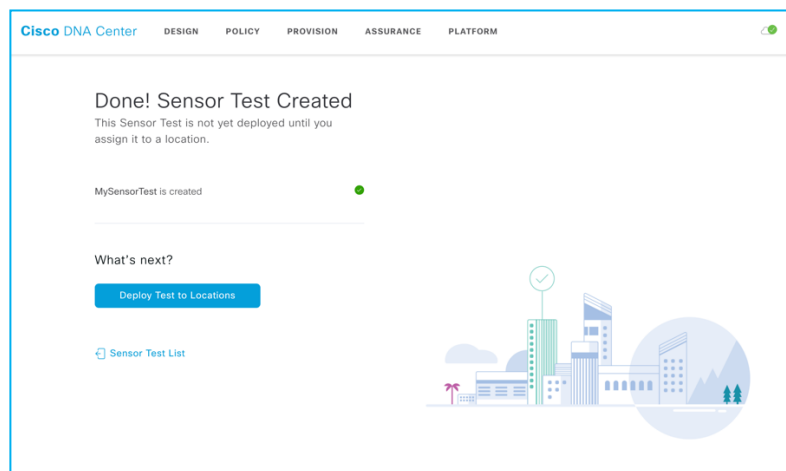
[Exit](#)

From this page, you can configure which band to test, the coverage threshold, and the number of test target APs per band.



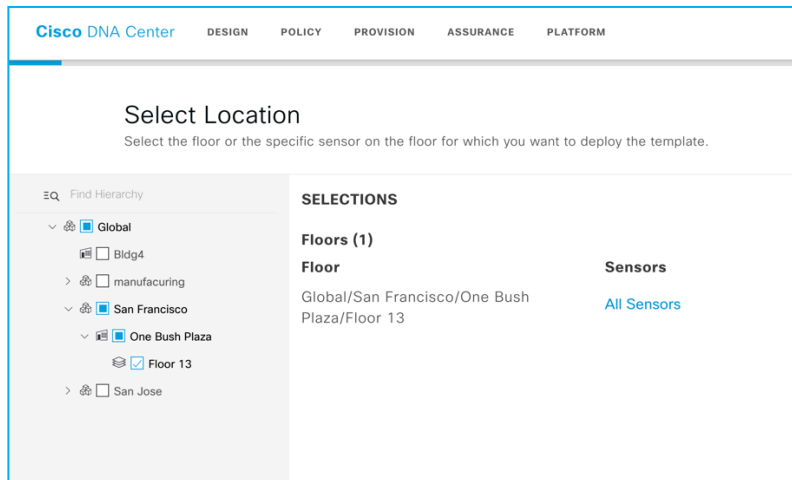
Finally, the **Sensor Test Template** page shows a summary of the configured sensor test options and allows you to review or go back to edit each section. This page also shows the estimated time that the test takes. This information is very important, because later, this estimated time is used to determine the sensor test interval.

After you create the sensor test template, you can move on to the next step, deploy a sensor to a location, or go back to the **Sensor Test List** page.

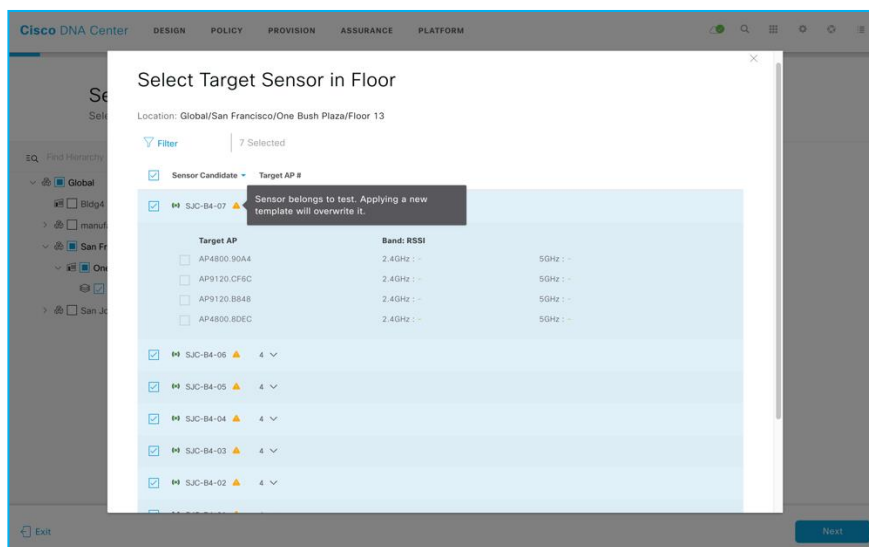


9. Click **Deploy Test to Location**. Then, assign sites to the recently configured sensor test template.

Create a Sensor Test Template



You can select all sensors on the floor by clicking **All Sensors**, or you can select individual sensors. Each sensor also shows a target AP list from which a target AP can also be selected. Starting with Cisco DNA Center 1.3.3, AP as a sensor is no longer supported, so an AP is not selectable as sensor candidate.



Each sensor can have only one sensor test template. So, if a selected sensor has already been assigned a sensor test template, a warning message is displayed.

10. Schedule sensor test.

From this page, the sensor test repeat interval and sensor test time and day can be configured.

For example, a sensor test can be configured to run only on weekdays or only on off-hours.

The sensor test repeat interval must always be higher than the estimated test cycle. If the sensor test estimated time is 25 minutes, the minimum repeat interval is 30 minutes. The **7 min** and **15 min** options are disabled from the drop-down list.

Finally, the sensor test can also be configured to run all the time. To configure this schedule, choose the **Continuous** radio button as the **Test Recurring** interval. This option needs to select with caution because it can overload the network or RADIUS server if lot of performance testing is included in this continuous test cycle.

A recommended best practice is to avoid setting the **Continuous** option when assigning sensor test templates to a large number of sites. Instead, use the **Continuous** option for select Sensors in suspicious locations. You can run some continuous sensor onboarding tests temporarily to verify successful network deployment.

11. Click **Deploy Test** and Cisco DNA Center assigns the new sensor test to a site. After that, whenever a new sensor is claimed and assigned to a specific floor, the sensor will automatically download a new sensor test template if a new or updated test template is discovered. This automation significantly simplifies the operation of sensors, because any newly claimed sensor can start testing automatically and instantly.

The newly added test is now displayed on the new **Sensor Dashboard** page. The sensor test results may not be updated immediately, because the sensor test is only updated after its first interval has passed.

The sensor runs a heartbeat process to Cisco DNA Center every minute through a dedicated backhaul channel (wired or wireless), and Cisco DNA Center informs the sensor of any new or updated sensor tests. Whenever a new or updated sensor test configuration is detected, the sensor will restart testing.

The previous sensor-driven tests are renamed to the legacy test suite in Cisco DNA Center 1.3.3.

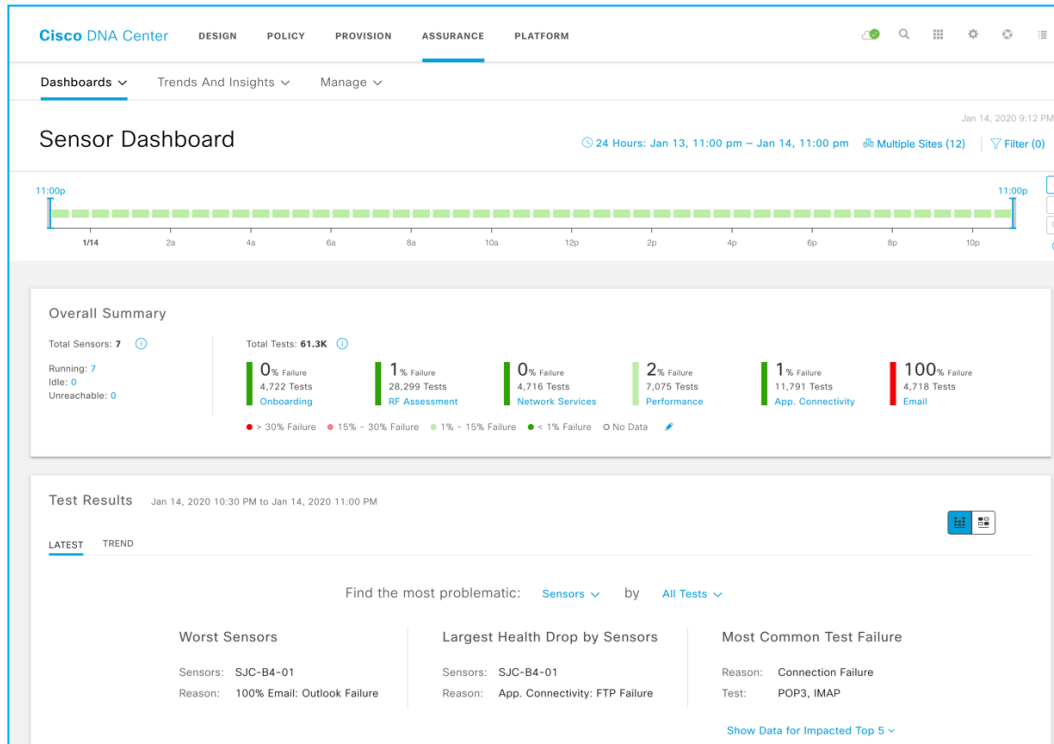
Monitor Sensor Health

Wireless Sensor Dashboard

Cisco DNA Center provides a global view of the wireless sensor test results in an intuitive heatmap view. This view allows you to determine potential issues and performance problems from an end-device point of view.

Choose **Assurance > Dashboards > Wireless Sensors**.

Wireless Sensor Dashboard



You can use the various location levels, SSIDs, and band filters to view information about specific sensors. To select an option, click its respective filter drop-down list. Click **Multiple Sites** for the hierarchical site view.

The **Wireless Sensor** dashboard is completely redesigned in software release 1.3.3 to provide intuitive navigation and drill-down view on each test result.

- **Overall Summary:** Provides a percentage and count of total and failed test. The dashlet also provides a breakdown of the types of sensor-driven tests that failed. Each test type (Onboarding, RF Assessment, Network Services, Performance, App Connectivity and Email Test) provides a drill-down view.
- **Test Result:** Provides a heatmap that is sorted by highest failure test type, a powerful location search bar, and top insight cards. The entire heatmap can be replaced with a dedicated insight card view. Each view can provide a further granular view by choosing a different level of location hierarchy (per-site, per-building, per-floor) or a different test type.

Color code Threshold Control test results are classified by 4 different color levels, and each color level has a customizable failure performance range.

Monitor Sensor Health

1% - 15% Failure ● < 1% Failure ○ No Data

Edit Threshold

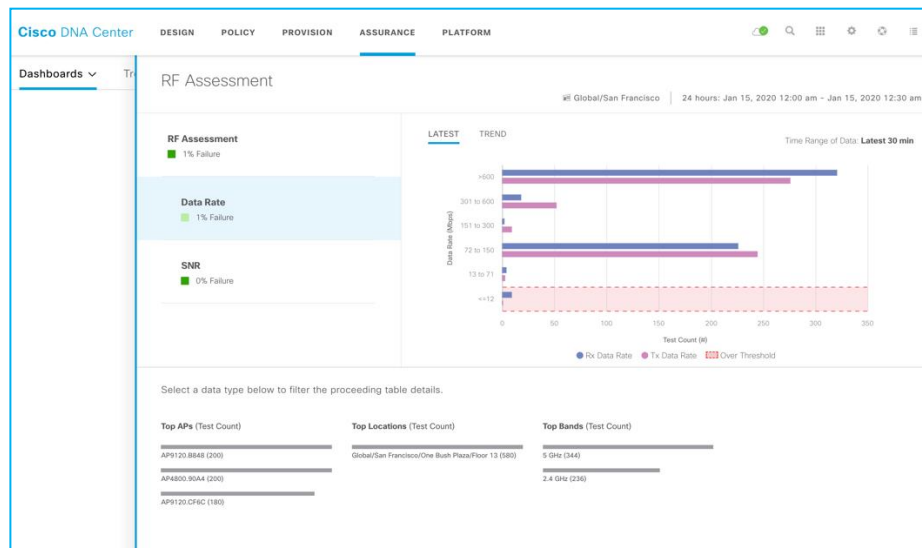
30	% -	100	% Failure
15	% -	30	% Failure
1	% -	15	% Failure
0	% -	1	% Failure

[Reset Settings to Default](#)

[Cancel](#) [Apply](#)

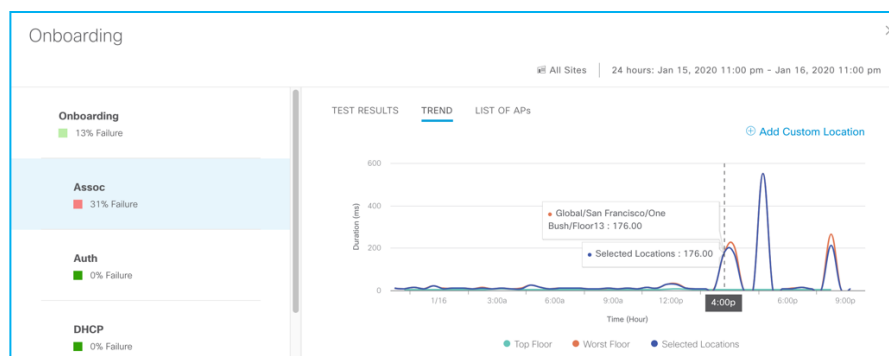
The test results heatmap view provides cognitive navigation and drill-down view. You can easily choose worst block or worst location + worst test type and identify the root cause of a problem from the drill-down detail page.

Sensor Test Drill-Down View



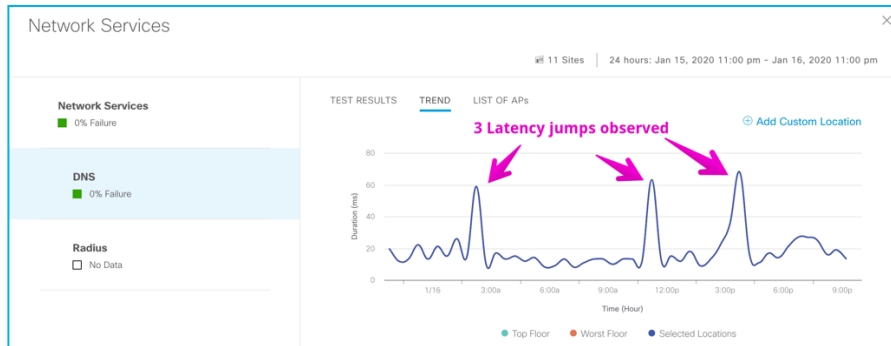
Each instance of a test result captures RF performance (RSSI, SNR, Tx/Rx Rate, Tx Retries) during the sensor test. For any test failure case, the drill-down view shows its failure reason.

When you click **TREND** from a drill-down detail chart, you can get various performance trend charts by test type.

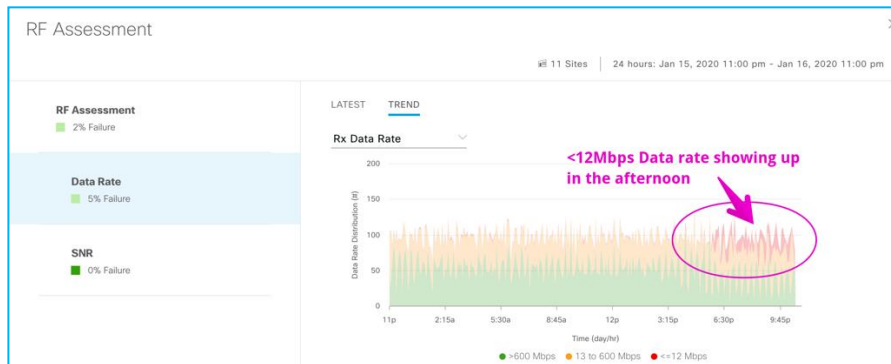


Monitor Sensor Health

The sensor test not only captures success or failure with a reason code, it is also continually capturing the transaction performance. It displays a comparison with best and worst floor at every 30-minute interval. You can also add any customer reference location and compare it with the selected location's result.

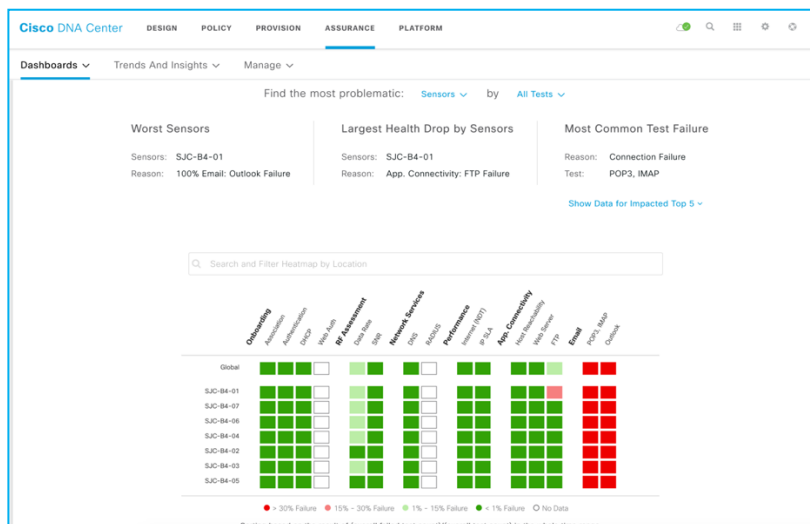


For example, this DNS test result shows 3 spikes on the DNS response during the last 24 hours.



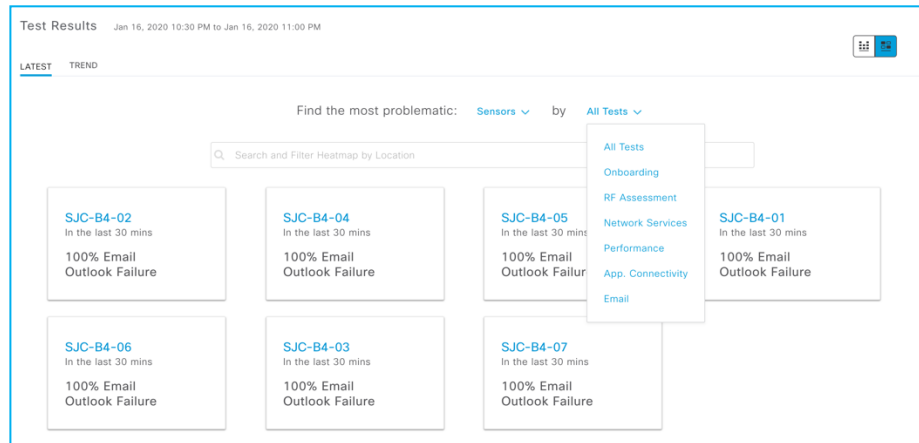
If you want to know more on the data rate trend, you can observe the DNS performance trend over time. The 3 levels provide easy identification of problematic time and percentage.

Sensor Test Result Heatmap View & Insight View



The sensor test results can be viewed by heatmap with various location hierarchies and test categories. The heatmap is always shown in sorted fashion, from worst (top) to best (bottom). The location granularity can be controlled by site, building, or floor level and can be as granular as each sensor level. At any location level, you can easily drill down into any cell and find out more details.

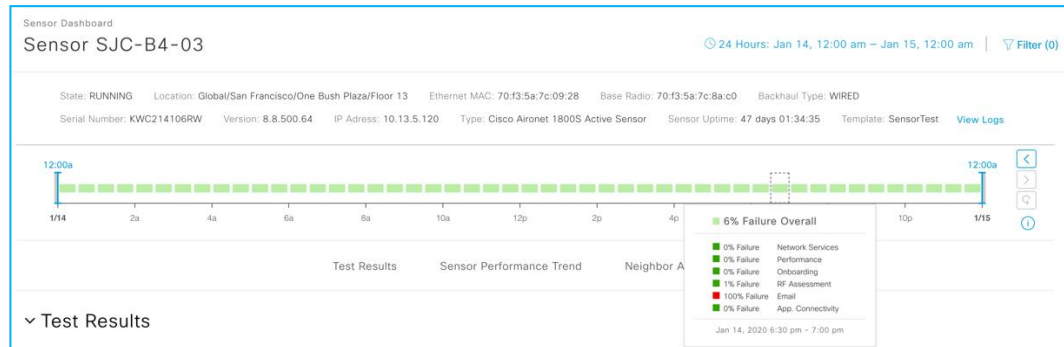
Each section also provides an insight view that highlights the most important findings from test result: worst location, largest health drop (highest failure rate increase), most common test failure across locations. The findings are expandable to show the top 5 locations of each section. You can also explore the dedicated insight view, which provides various card views and is also mapped to the selected location level and test category.



You can zoom into each sensor by clicking the sensor name.

Sensor 360

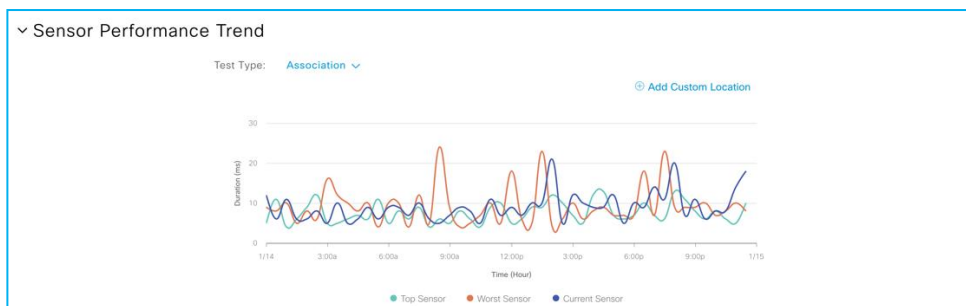
The **Sensor 360** page displays all the details of a specific sensor device, from device details to sensor test results with heatmap and network time-travel bar, sensor performance trend and neighbor AP list with floor maps, event logs and so on.



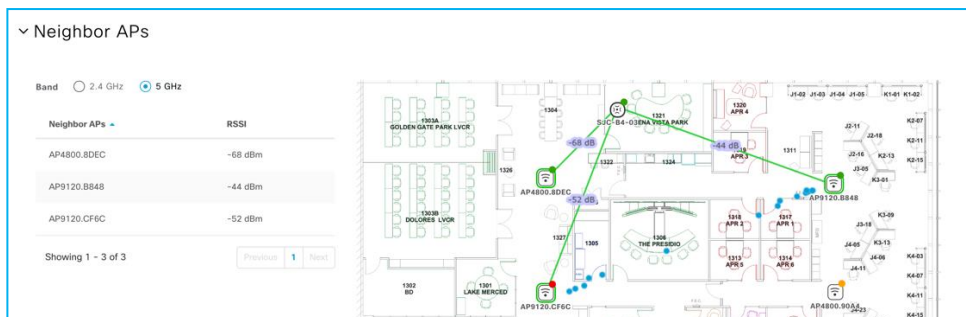
The **Sensor 360** page also includes sensor test results bar based on test success percentage rate. This page has same navigation and filter rules as wireless client. The **View Logs** link is used to access sensor troubleshooting information.



The Sensor 360 Heatmap is designed with the same philosophy as the Sensor Dashboard but the Sensor 360 Heatmap provides an additional level of detail by showing the per AP test result.



The Sensor Performance Trend chart shows performance test of each sensor test. It's designed mainly for comparative analytics by providing a comparison trend between the currently selected sensor and the worst and best sensor test results. In addition, you can add any location so that you can compare current sensor vs. a location-specific average value.



The Neighbor AP view provides all the neighbor scanning AP results and shows a visual relationship between the sensor location and the deployed AP location.

Sensor Global Issues

The screenshot shows the Cisco DNA Center Assurance page. The main table lists sensor issues, and a side panel shows details for 'Sensors - DHCP Failures'.

Issue Name	Enabled	Priority	Global	Current
Sensor - Slow Authentication during Onboarding	Yes	P4	Yes	Default
Sensors - Radius Reachability Slow	Yes	P3	Yes	Default
Sensors - Speed Test HTTP Error	Yes	P3	Yes	Default
Sensors - Default Gateway Failed	Yes	P3	Yes	Default
Sensors - DHCP Failures	Yes	P2	Yes	Default
Sensors - DNS Resolution Failed	Yes	P3	Yes	Default
Sensors - DNS server Reachability Failed	Yes	P3	Yes	Default
Sensors - DNS Server Slow Response	Yes	P3	Yes	Default
Sensors - Failed Association during Onboarding	Yes	P3	Yes	Default
Sensors - Failed Authentication during Onboarding	Yes	P3	Yes	Default
Sensors - First Hop Slow Response	Yes	P3	Yes	Default
Sensors - FTP Reachability Slow	Yes	P3	Yes	Default

The side panel for 'Sensors - DHCP Failures' shows the following details:

- Multiple sensors failed to get an IPv4 address
- Enabled: ☒
- Priority: P2
- Last Modified: --
- View Default Setting

When two or more sensors on the same floor fail a test in a 30-minute period, the sensor can raise an issue based on the failed test type. These sensor issues are all global issues, meaning that the sensor issue from any floor is escalated and shown in the first **Issue Dashboard** page.

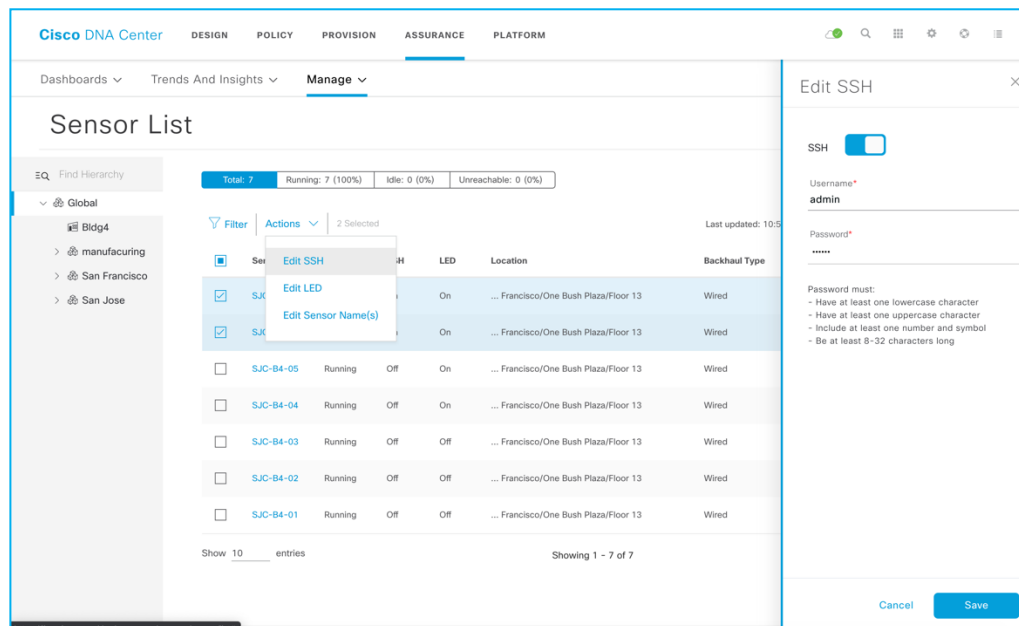
You can customize the priority or turn on or off any sensor issue type. In Cisco DNA Center Release 1.3.3, sensor issues are also exportable from the **Issue Dashboard** page.

Troubleshooting

Sensor Command Line Interface

For troubleshooting the sensor, you can use a console cable, SSH, or a sensor support bundle that is retrievable from the **Sensor 360** page.

The sensor supports SSH but fully enabled SSH is disabled by default. (Only limited Day-0 SSH is enabled before the sensor is connected to Cisco DNA Center.) After the sensor is provisioned in Cisco DNA Center, Day-0 SSH is disabled, and you can use the **Sensor List** page to enable the SSH service on the sensor.



You can change the username and password of the sensor using the **Edit SSH** action. The username and password that you configure is applied on both SSH and console access.

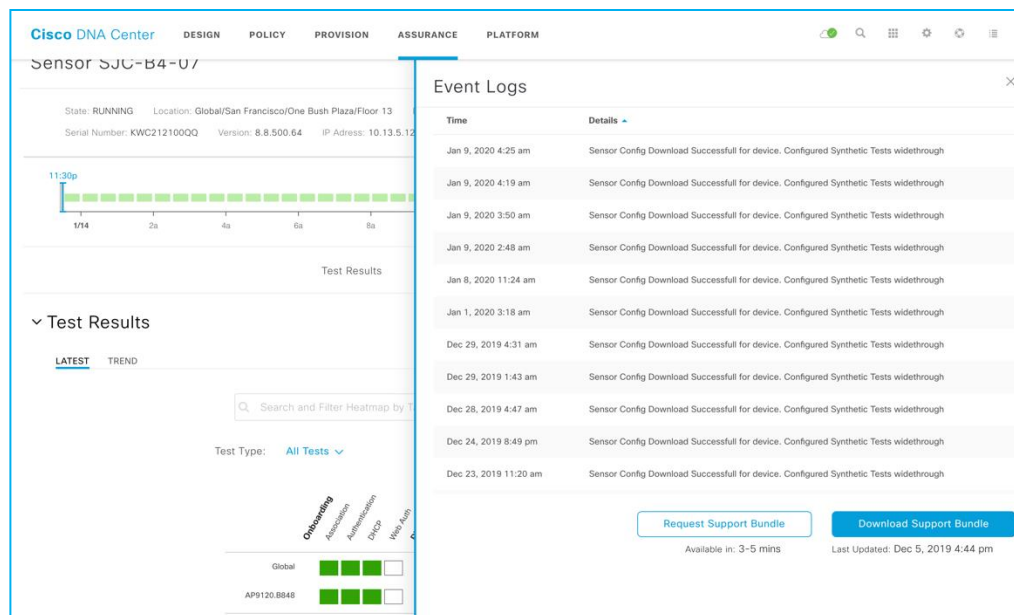
Sensor specific commands have a prefix of `show/config dot11 sensor` command line, as shown in the following example:

```
Sensor-5C98>show dot11 sensor
  heartbeat Show WSA Agent Heartbeat Information
  neighbors Show dot11 sensor neighborlist
  prov-ssid Show dot11 sensor provisioning SSID list
  route      Show dot11 sensor route
  scan       Show WSA Scanned Information
  stats      Show dot11 sensor statistics
  synthetic  Show WSA Synthetic Tests Information
  test       Show WSA Test Information
  wpas-log   Show dot11 sensor WPA-Supplicant log
  wsa-log    Show dot11 sensor WSA log
```

Event Log and Sensor Support Bundle

Sensor troubleshooting information is available from the **Sensor 360** page.

From the **Sensor 360** page, the **Event Log** page shows the sensor event logging viewer and provides a downloadable sensor TAC support bundle.



The sensor support bundle can be retrieved from the sensor and downloaded to Cisco DNA Center by clicking the **Request Support Bundle** button. Once the downloadable support bundle becomes available, an updated time under the **Download Support Bundle** button is displayed. The support bundle tar file includes all the sensor logging information that is often requested by Cisco TAC, and you can easily attach it to your communication with Cisco TAC.

Reset Sensor Configuration

To reset the sensor configuration to the factory default, enter the following command:

```
# clear dot11 sensor
```

The sensor also provides a hard reset button on its side panel. This reset button can be used to reset the sensor back to its factory default settings and to erase all configuration, including any static DNA Center IP addresses.

To reset the network sensor to the factory default configuration, press and hold the **Reset** button for a minimum of 20 seconds. The network sensor configuration files are cleared.



Show Heartbeat Status

A heartbeat between Cisco DNA Center and the sensor occurs every 60 seconds. Run the following command to see the status and last success time of the heartbeat. If there is a failure, confirm connectivity to Cisco DNA Center.

```
# show dot11 sensor heartbeat status
```

Failing condition:

```
AP70F3.5A7A.5C98#show dot11 sensor heartbeat status
AP70F3.5A7A.5C98# // No response or message
```

```
# show dot11 sensor test config

Test Config Received Time: 2019-05-25 22:20:44.912481
{
  "advancedConfig": {
    "rssiThreshold": -75
  },
  "testConfig": [
    {
      "name": "Onboarding",
      "bands": "BOTH",
      "scheduleInDays": 0,
      "connection": "WIRELESS",
      "frequency": {
        "value": 1,
        "unit": "HOURS"
      },
      "ssids": [
        {
          "username": "Sensor2",
          "validTo": 0,
          "layer3webAuthsecurity": null,
          "numAps": 0,
          "id": 0,
          "authTypeRcvd": null,

```

The following example shows the configuration that the sensor received from Cisco DNA Center through the WLC.

```
# show dot11 sensor test result all
Test No: 1.1, Name: Onboarding, Time: 2019-05-25 22:52:10.931352
Test Results: {
  "macAddress": "70:f3:5a:78:6b:60",
  "testCompleted": "no",
  "type": "DEDICATED",
  "connectivityStats": {
    "wireless": {
      "status": "SUCCESS",
      "channelWidth": 20,
      "connectionTime": 8,
      "bssid": "70:69:5A:51:3F:A0",
      "txDataRate": 78000,
      "responseTimesInMillis": {
        "probeRequest": 53,
        "authenticationRequest": 84,
        "handshake": 1477,
        "associationRequest": 36
      },
      "snr": 42,
      "rssi": -40,
      "channel": 1
    },
  },

```

The following example shows the results of the sensor test.

```
# show dot11 sensor synthetic work list
```

Group	Suite	SSID	Access Point	Radio
1	Global/San Francisco/One Bush St/Flr13:!	_1800S_Wired	@CorpSSID	70:69:5a:51:3f:a0
802.11b				
	RSSI	Frequency	Skip Repeat	Min Time Max Time Avg Time

```

=====
-42 dBm 1 HOURS          0    0          01:82.39 01:82.39 01:82.39
=====

Test  Name          Pass  Fail  Latest  Min Time  Max Time  Avg Time
=====
1    Onboarding      1    0    Pass    00:15.05  00:15.05  00:15.05
2    IpslaSender      0    1    Fail    N/A
3    DNS              1    0    Pass    00:05.46  00:05.46  00:05.46
4    Ping             1    0    Pass    00:07.14  00:07.14  00:07.14
5    Speed            1    0    Pass    00:43.30  00:43.30  00:43.30
6    WebServer        1    0    Pass    00:01.14  00:01.14  00:01.14
=====

```

The following example shows details for each test that the sensor will execute.

```

# show dot11 sensor stats.

## Network Assurance Sensor Statistics ##
WSA Status: Enabled
NA Connectivity: Connected
NA Connectivity I/F: Wired http
NA Server URL: https://10.13.1.100
Auth Type: EAP
HTTP Proxy IP: PROXY_IP
Backhaul SSID: SensorBH
Id-token:
Port: PORT
Total Test Cases Run: 55
Successful Test Cases: 51
Failed Test Cases: 4
Network Assurance 5G Radio Statistics
-----
Host Rx K Bytes: 1063804
Host Tx K Bytes: 766328
Unicasts Rx: 1528921
Unicasts Tx: 746511
Broadcasts Rx: 0
Broadcasts Tx: 19
Beacons Rx: 3250
Beacons Tx: 0
Multicasts Rx: 0
Multicasts Tx: 0
CRC errors: 4512
TX retries: 24686

```

Look for **Total Test Cases Run**, **Successful Test Cases**, and **Failed Test Cases**. These results give an indication of how many tests the sensor has performed and the overall status of those tests. Note the values also include radio stats and does show you if Cisco DNA Center connectivity is enabled.

```
# show dot11 sensor scan list
```

This shows the APs that the sensor can hear and at what signal level. Only APs with RSSI of -75 or higher are tested.

```
# show dot11 sensor wsa-log
```

Gives the complete log of all the events.

```
# debug wsa debug
```

Use 'term mon' to view the full debug output from the Web Security Appliance (WSA) debug.

PNP related CLIs (useful during PnP provisioning phase)

<pre>#config dot11 sensor pnp ip 192.168.0.100</pre>	Prime DNAC's IP address (192.168.0.100) statically
<pre># show pnp info PI version: 1.8.0.dev20 PD version: 1.5.2.dev2</pre>	Show the pnp agent version.
<pre># show pnp status</pre>	Show the pnp status.

Detailed Troubleshooting Commands Output

```
# show dot11 sensor heartbeat status

Heartbeat Status: Success, Count: 1787
SSH status: Disabled
Heartbeat Version: 3
Heartbeat Last Success Time: 2019-05-25 23:10:08.567167
```

Useful Links

- *Cisco DNA Center Admin Guide*
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-3-0/admin-guide/b_cisco_dna_center_admin_guide_1_3_3_0.html
- *Cisco DNA Center Release Notes*
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center/1-3-3-0/release-notes/b_cisco_dna_center_rn_1_3_3_0.html
- *Cisco DNA Assurance User Guide 1.3.3.0 Manage Sensors and Sensor-Driven*
https://www.cisco.com/c/en/us/td/docs/cloud-systems-management/network-automation-and-management/dna-center-assurance/1-3-3-0/b_cisco_dna_assurance_1_3_3_0 Ug/b_cisco_dna_assurance_1_3_2_0 chapter_01010.html
- *Solution Guide for Cisco Network Plug & Play*
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#con_115699
- *Cisco Series Console Adapter Cable AIR-CONSADPT= Guide*
https://www.cisco.com/c/en/us/td/docs/wireless/access_point/console_adptr/guide/air_console_adptr.html