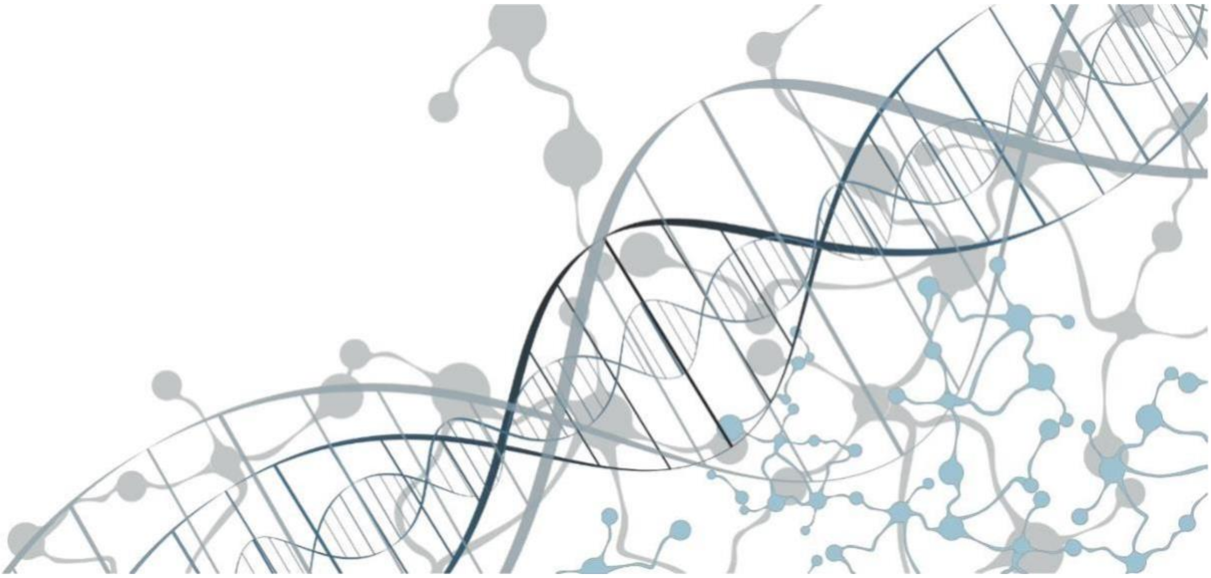
Cisco Aironet Active Sensor Deployment Guide



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

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

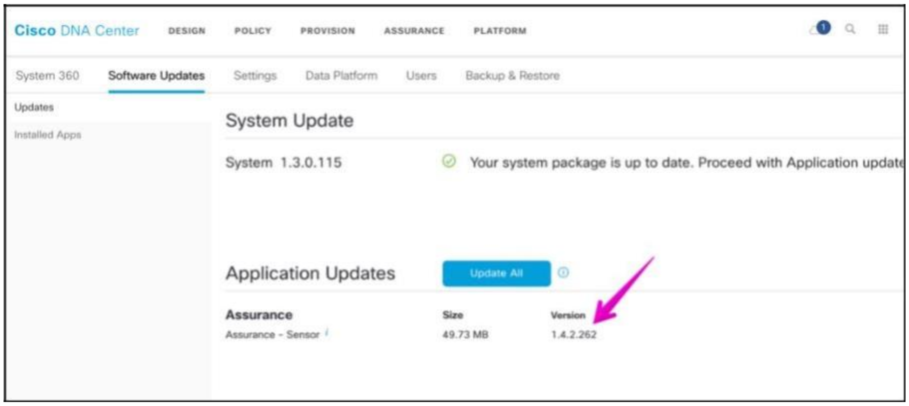
Sensor Suggested Software Release	Cisco DNA Center Software Release
1.3.3.0	Suggested for Cisco DNA Center 1.3.3.x
1.3.1.2	Suggested for Cisco DNA Center 1.3.1.2 or later 1.3.1.x
8.8.263.0	Suggested for Cisco DNA Center 1.3.0.3 or earlier (example: 1.2.x)

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



System Update

System 1.3.0.115 — Your system package is up to date. Proceed with Application update

Application Updates

Assurance	Size	Version
Assurance - Sensor	49.73 MB	1.4.2.262

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.

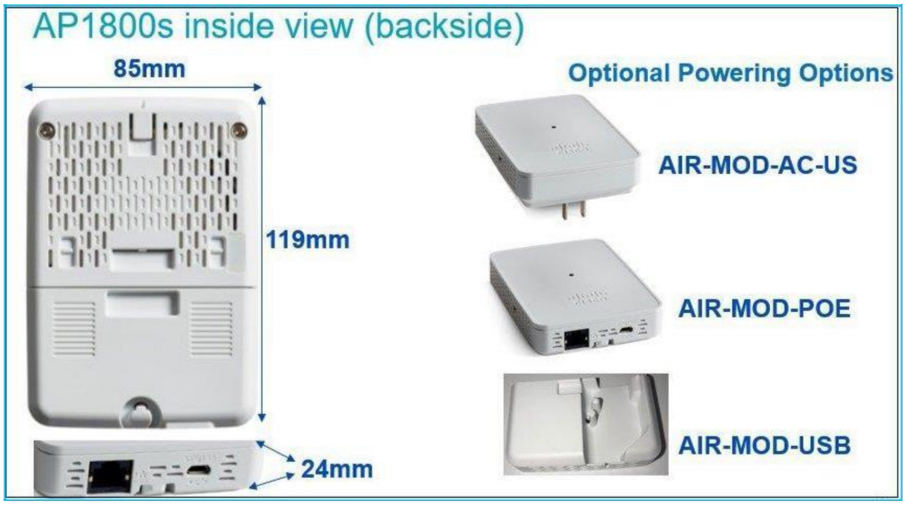
Cisco 1800S Sensor

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”

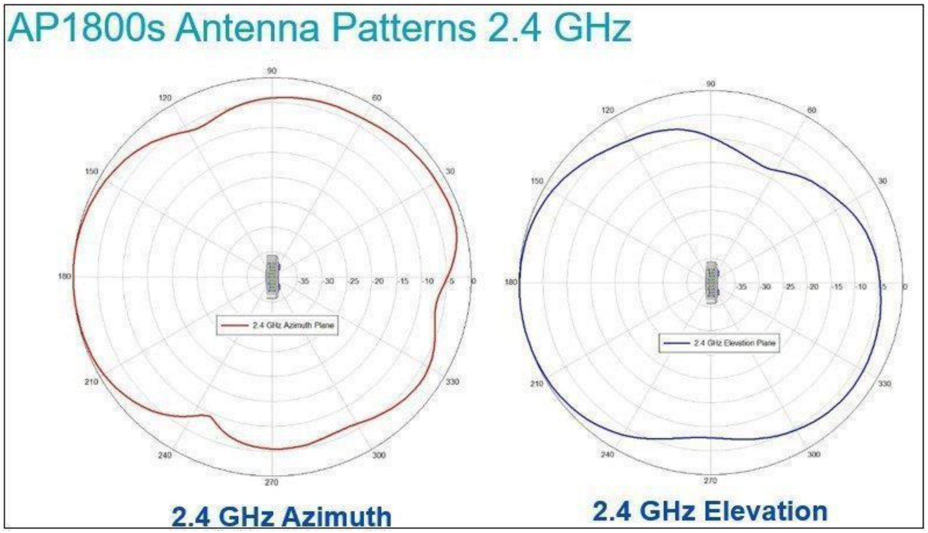
Without a power over Ethernet (PoE) module, power can be supplied from a local 2.5 ampere/5-volt USB port, using a micro-USB Type-B connector. (There is USB Type-C connector, but it is dedicated for the PoE module connection.) Additionally, there are modules that allow for a direct AC power supply, as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

Cisco 1800S Sensor - Backside View

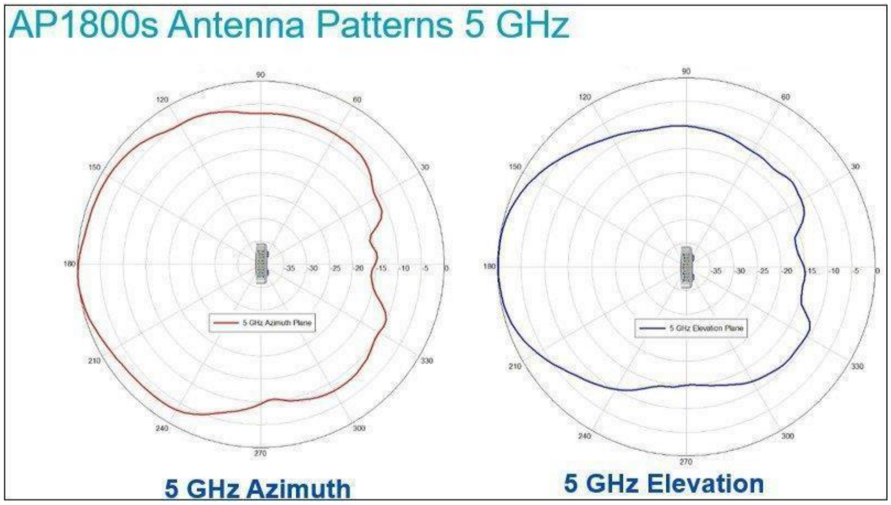


The following figures show the antenna system on the sensor.

Cisco 1800S Sensor - Antenna Pattern 2.4 GHz



Cisco 1800S Sensor - Antenna Pattern 5 GHz



Cisco 1800S Sensor and Accessory Product IDs (PIDs)

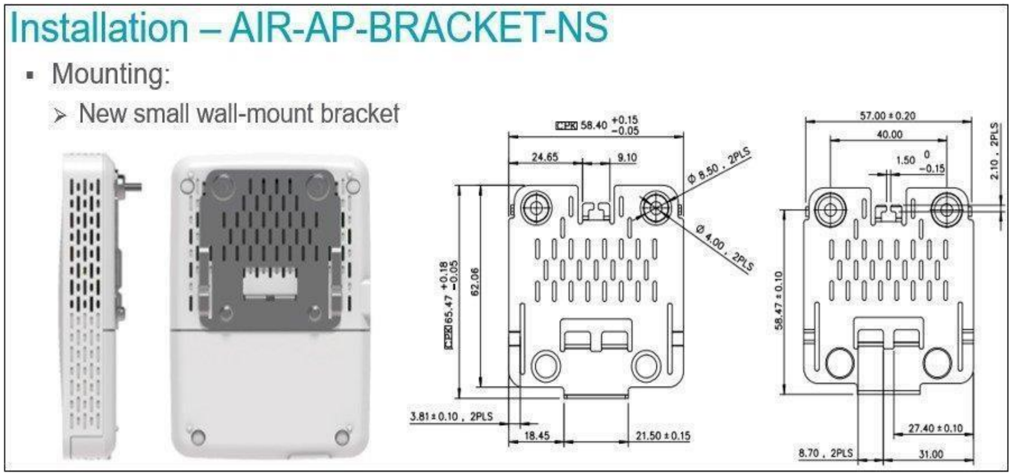
Name	Product ID
Cisco 1800S Sensor	AIR-1800S-x-K9
PoE with 1 G Ethernet Module	AIR-MOD-SPOE
USB Adapter Power Module – US Plug Only	AIR-MOD-USB-US=
USB Adapter Power Module – Rest of World (includes bag of 5 international plugs)	AIR-MOD-USB-RW=
Wall Mount Bracket Kit	AIR-AP-BRAKET-NS
Cisco 1800S Console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

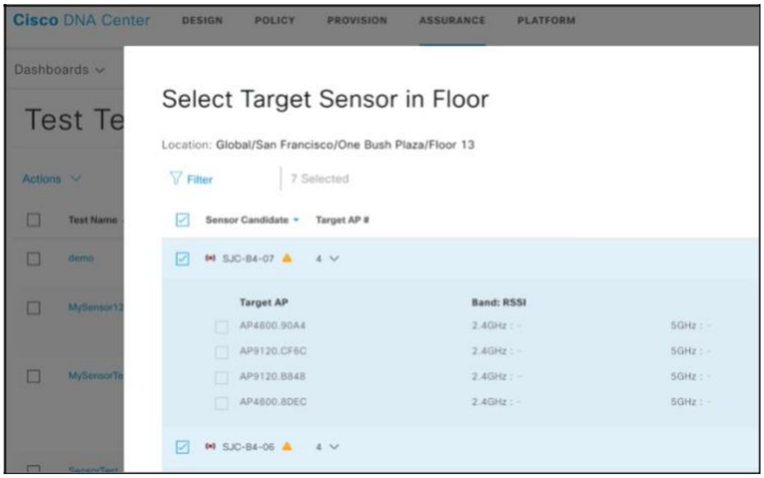
Cisco 1800S Sensor - Mounting



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.



Select Target Sensor in Floor

Location: Global/San Francisco/One Bush Plaza/Floor 13

Filter | 7 Selected

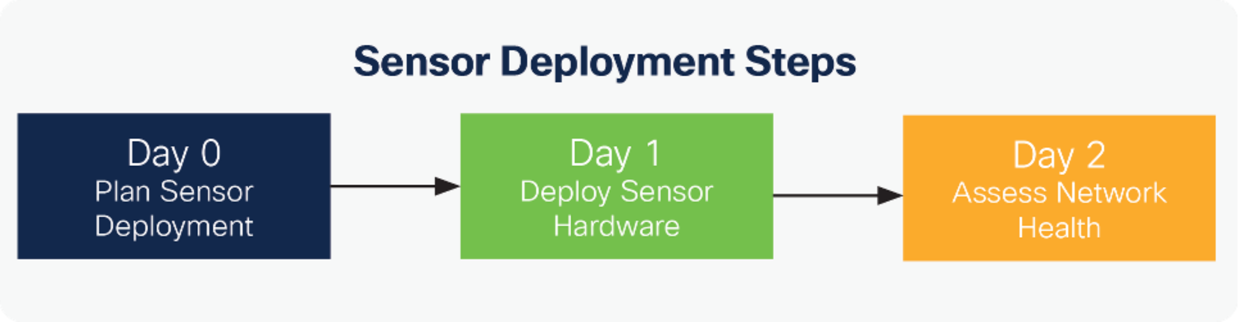
☑	Sensor Candidate	Target AP #
☑	SJC-B4-07	4

	Target AP	Band: RSSI	
□	AP4800.90A4	2.4GHz : -	5GHz : -
□	AP9120.CF6C	2.4GHz : -	5GHz : -
□	AP9120.B848	2.4GHz : -	5GHz : -
□	AP4800.8DEC	2.4GHz : -	5GHz : -

☑	SJC-B4-06	4

Software deployment checklist

Sensor deployment involves the following steps.



1. Plan the number of sensors that will be deployed per site and the location.

    a. To determine the number of sensors to deploy and their position of deployment, we must consider the following.

        i. During each test cycle, the sensor can test up to 5 surrounding APs with the highest RSSI. This means that we must first analyze each location's floor map to determine which potential sensor deployment locations will allow every AP on the floor to be tested.

        ii. Determine the scope of your wireless tests from a frequency perspective, and take into consideration whether you plan to test just 2.4GHz, just 5GHz, or both. A 2.4GHz signal will have a further range compared to 5GHz, and the sensor deployment may differ based on how your network is configured.

        iii. Pay attention to each floor's physical layout and where the RF signal can easily travel vs. not. For example, if your building has many solid walls or areas that easily reflect RF signals, take it into account during the planning phase. Consider visiting the potential sites of deployment and analyze whether you're able to see each of the broadcasted SSIDs/BSSIDs from each of the APs you'd like to test. If you're able to see all of these SSIDs/BSSIDs within the RSSI range you plan to configure, this could be an ideal location for sensor testing.

        iv. Remember that the Aironet Active Sensor's goal is to test the wireless network from the perspective of a client. While all prior points are critical, it is also essential to place your sensors in a location where laptops or phones would typically be used. For example, placing a sensor in an area where a large amount fo employees work would be more beneficial to understanding the effectiveness of your wireless network than compared to putting the sensor in an area where there is no one.

2. Configure the network infrastructure necessary for Sensor deployment and testing.

    a. Create a VLAN planned for sensor use on a switch that can reach Cisco DNA Center.

    b. Configure a Dynamic Host Configuration Protocol (DHCP) or DNS server for the created VLAN, and include Plug and Play (PnP) discovery method details (option 43 or pnpserver.cisco.com DNS entry) to allow the sensor to discover Cisco DNA Center during provisioning.

    c. Optional planned PnP: Create and claim PnP profiles on Cisco DNA Center for the sensors you plan to install on day 1.

    d. Prepare the sensor test target servers such as AAA, email, and FTP, and ensure that the sensor device network has direct access to these.

    e. Create and deploy a sensor test template to the desired sites in Cisco DNA Center.

    f. Option 1 – wired backhaul: Set up a wired network between the sensor and Cisco DNA Center.

    g. Option 2 – wireless backhaul: Create a CiscoSensorProvisioning SSID on the wireless controller.

Day 1: Deploy sensor hardware

1. Install the sensors in the planned locations.
    a. Connect the sensors through PoE, USB, or AC (depending on whether you're planning to use a wired or wireless backhaul) to have them begin PnP discovery to Cisco DNA Center once they receive IP addresses from the DHCP server.
    b. Once the sensor appears in the PnP page of Cisco DNA Center, claim the sensor to a site and verify in the sensor list page that the claim was successful.
    c. Optional image upgrade: If the sensors are not running the latest image, mark the latest image within the Software Images page as the golden image, then upgrade the sensors through the Inventory page.
    d. If not already assigned in day 0, create and assign test templates to specific sites or sensors to begin testing.

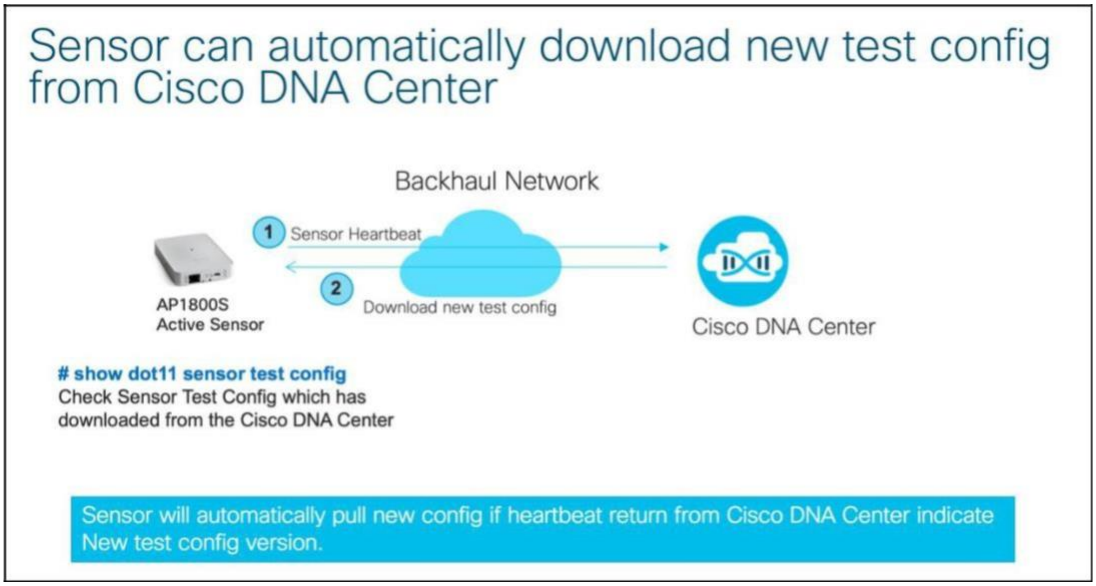
Day 2: Assess network health

1. Observe the sensor test results through the Wireless Sensors dashboard and Sensor 360 page.
    a. Troubleshoot any sensor issues using the Sensor 360 page's event log feature.

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

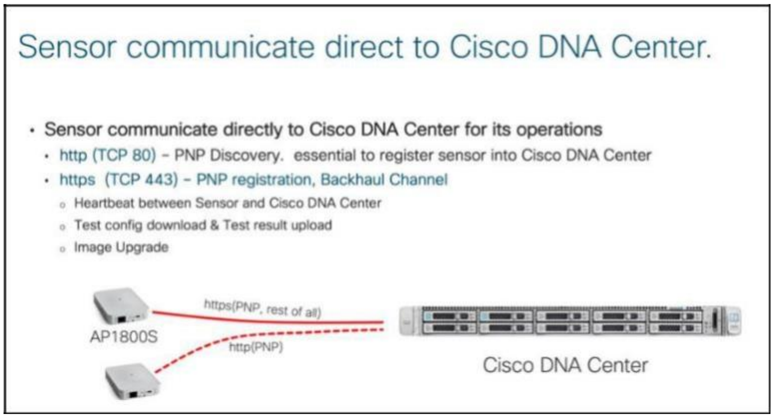


Sensor can automatically download new test config from Cisco DNA Center

# show dot11 sensor test config
Check Sensor Test Config which has downloaded from the Cisco DNA Center

Sensor will automatically pull new config if heartbeat return from Cisco DNA Center indicate New test config version.

Network Port Between Sensor and Cisco DNA Center



Sensor communicate direct to Cisco DNA Center.

- Sensor communicate directly to Cisco DNA Center for its operations
  - http (TCP 80) – PNP Discovery. essential to register sensor into Cisco DNA Center
  - https (TCP 443) – PNP registration, Backhaul Channel
    - Heartbeat between Sensor and Cisco DNA Center
    - Test config download & Test result upload
    - Image Upgrade

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, PNPSERVER. The last resort is manual CLI input via console or SSH.

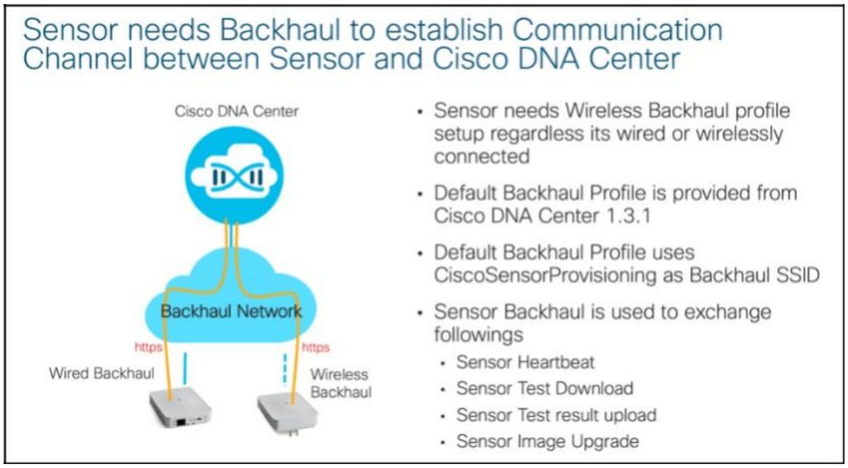
Preparation: Network Connectivity Between Sensors and Cisco DNA Center

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



Sensor needs Backhaul to establish Communication Channel between Sensor and Cisco DNA Center

- Sensor needs Wireless Backhaul profile setup regardless its wired or wirelessly connected
- Default Backhaul Profile is provided from Cisco DNA Center 1.3.1
- Default Backhaul Profile uses CiscoSensorProvisioning as Backhaul SSID
- Sensor Backhaul is used to exchange followings
  - Sensor Heartbeat
  - Sensor Test Download
  - Sensor Test result upload
  - Sensor Image Upgrade

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 SD-Access/fabric environment, the fabric edge that serves the sensor connection has a Maximum Transmission Unit (MTU) that will be automatically configured to 9100.

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.

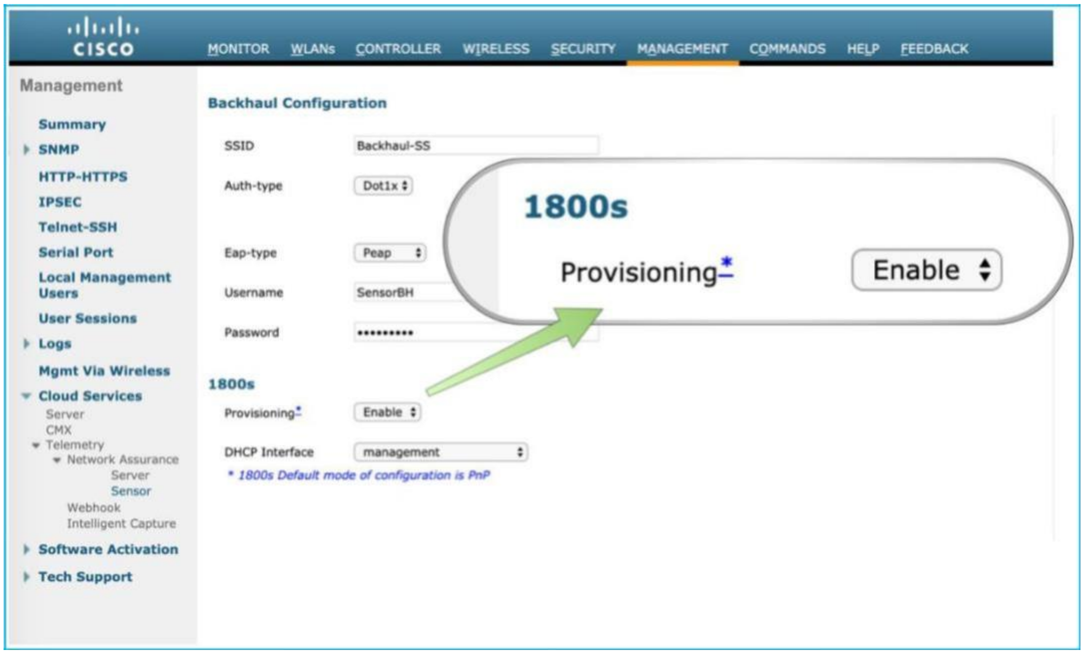
To solve this problem, the AP and sensor use a factory installed SSID named *CiscoSensorProvisioning*. This SSID is known to both the wireless controller and the sensor from a factory shipment level.

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



Backhaul Configuration

SSID: Backhaul-SS

Auth-type: Dot1x

Eap-type: Peap

Username: SensorBH

Password: •••••••••

1800s

Provisioning*: Enable

DHCP Interface: management

* 1800s Default mode of configuration is PnP

1800s

Provisioning*: Enable

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.

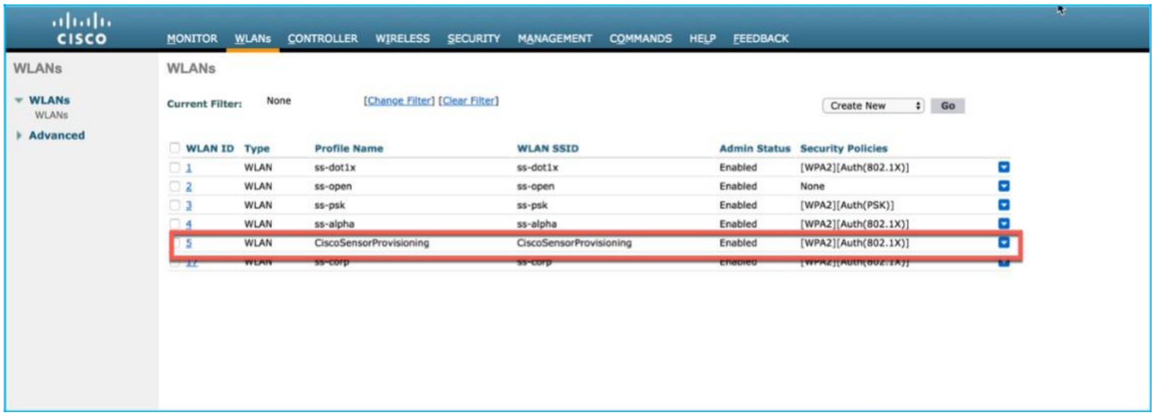
   — The sensor can connect to the Cisco AP and use it to reach Cisco DNA Center.

   — 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



WLANs

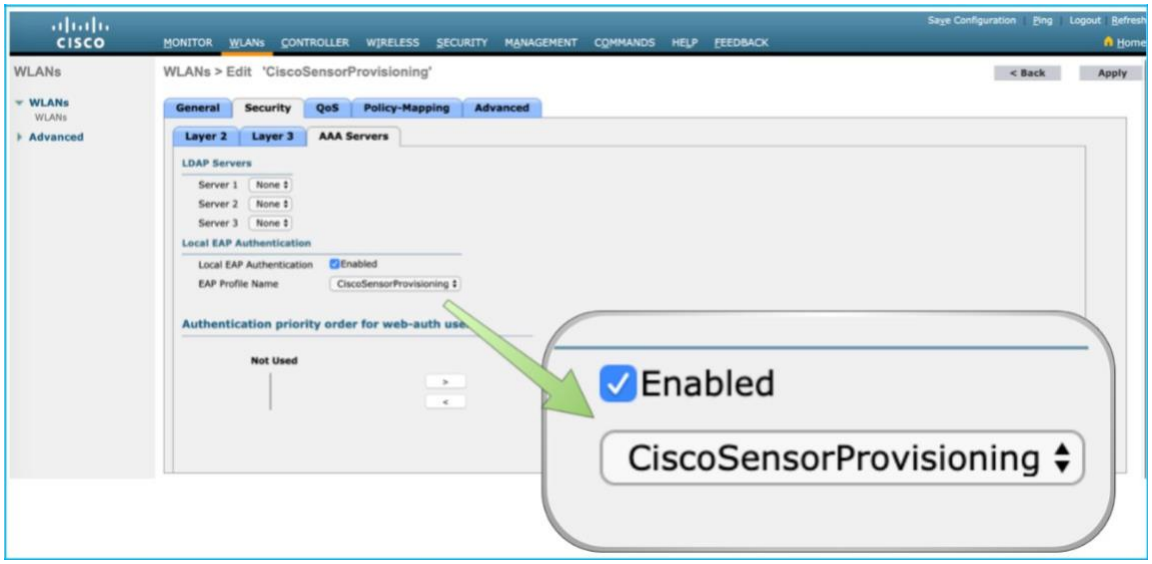
Current Filter: None [Change Filter] [Clear Filter]

	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



WLANs > Edit 'CiscoSensorProvisioning'

LDAP Servers

Server 1 None

Server 2 None

Server 3 None

Local EAP Authentication

Local EAP Authentication ☑ Enabled

EAP Profile Name CiscoSensorProvisioning

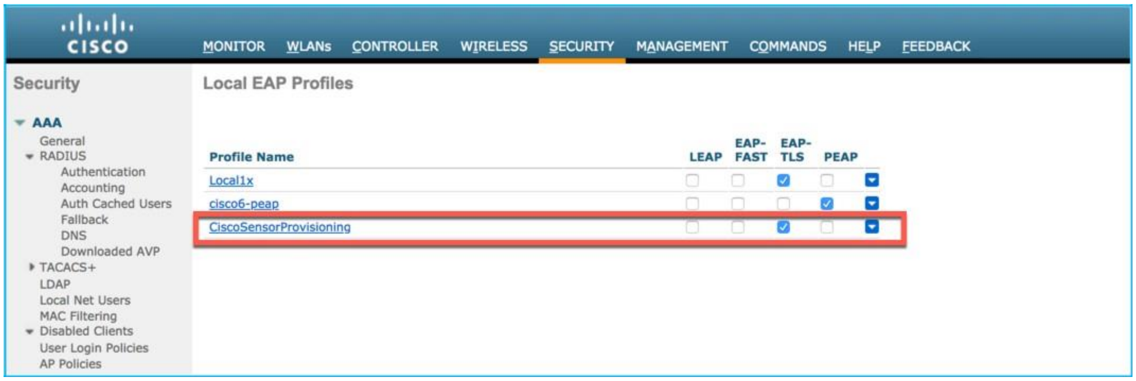
Authentication priority order for web-auth use

☑ Enabled

CiscoSensorProvisioning

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



Local EAP Profiles

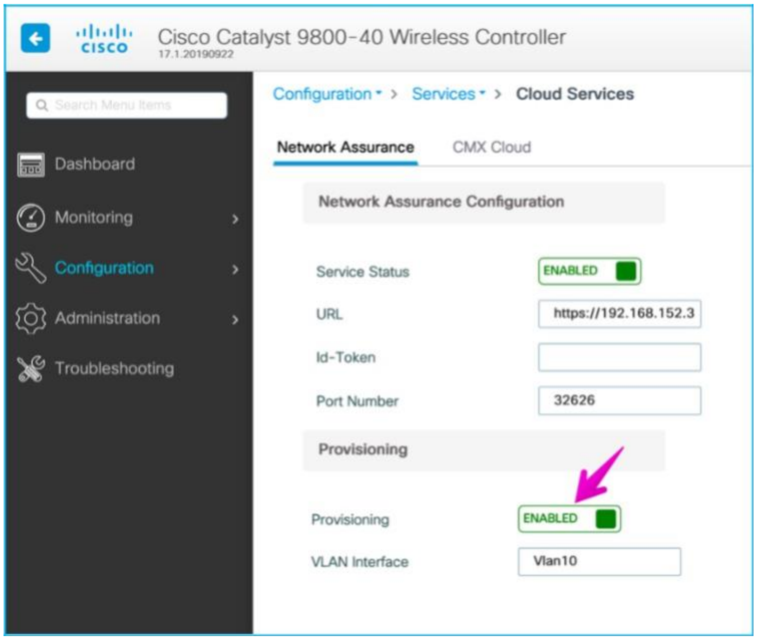
Profile Name	LEAP	EAP-FAST	EAP-TLS	PEAP
Local1x	□	□	☑	□
cisco6-peap	□	□	□	☑
CiscoSensorProvisioning	□	□	☑	□

Note:

- The CiscoSensorProvisioning SSID does not broadcast SSID over the air. It's hidden by default; the sensoe can discover and connect to this hidden CiscoSensorProvisioning SSID.
- If your sensor is using a wireless backhaul method, you must keep the CiscoSensorProvisioning SSID enabled at all times.

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**.



Network Assurance Configuration

Service Status: ENABLED

URL: https://192.168.152.3

Id-Token:

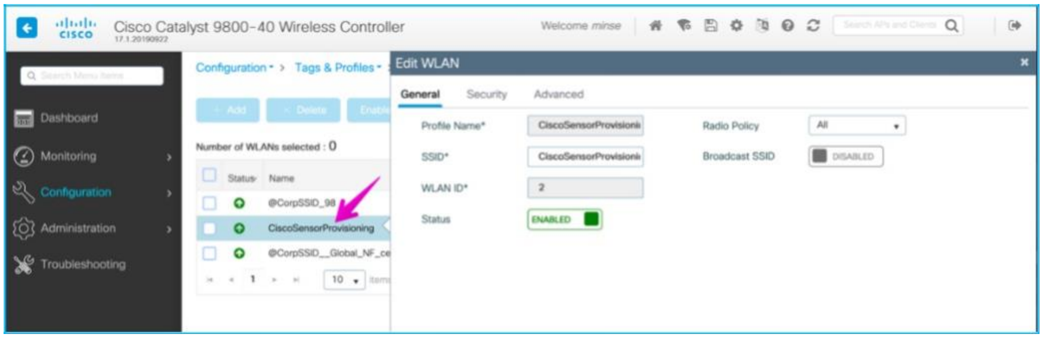
Port Number: 32626

Provisioning

Provisioning: ENABLED

VLAN Interface: Vlan10

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



Profile Name*: CiscoSensorProvisioni

SSID*: CiscoSensorProvisioni

WLAN ID*: 2

Status: ENABLED

Radio Policy: All

Broadcast SSID: DISABLED

Note:

- 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.
- If your sensor is using a wireless backhaul method, you must keep the CiscoSensorProvisioning SSID enabled at all times.

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
```

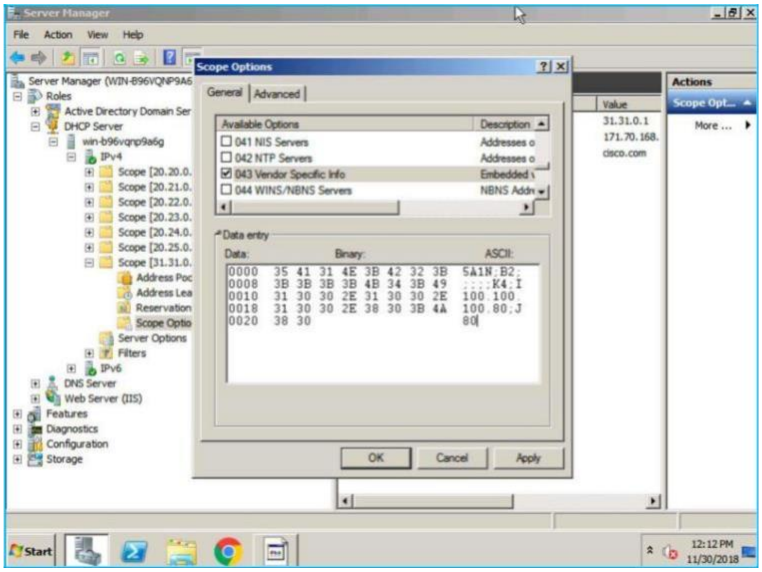
When the sensor receives its own IP address from the DHCP server, it also gets the Cisco DNA Center IP address through the DHCP Option 43 field.

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



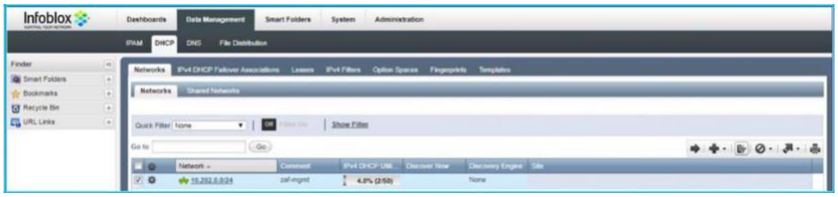
Available Options	Description
□ 041 NIS Servers	Addresses o
□ 042 NTP Servers	Addresses o
☑ 043 Vendor Specific Info	Embedded v
□ 044 WINS/NBNS Servers	NBNS Addr

```
Data:     Binary:                     ASCII:
0000  35 41 31 4E 3B 42 32 3B   5A1N;B2;
0008  3B 3B 3B 3B 4B 34 3B 49   ;;;;K4;I
0010  31 30 30 2E 31 30 30 2E   100.100.
0018  31 30 30 2E 38 30 3B 4A   100.80;J
0020  38 30                     80
```

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

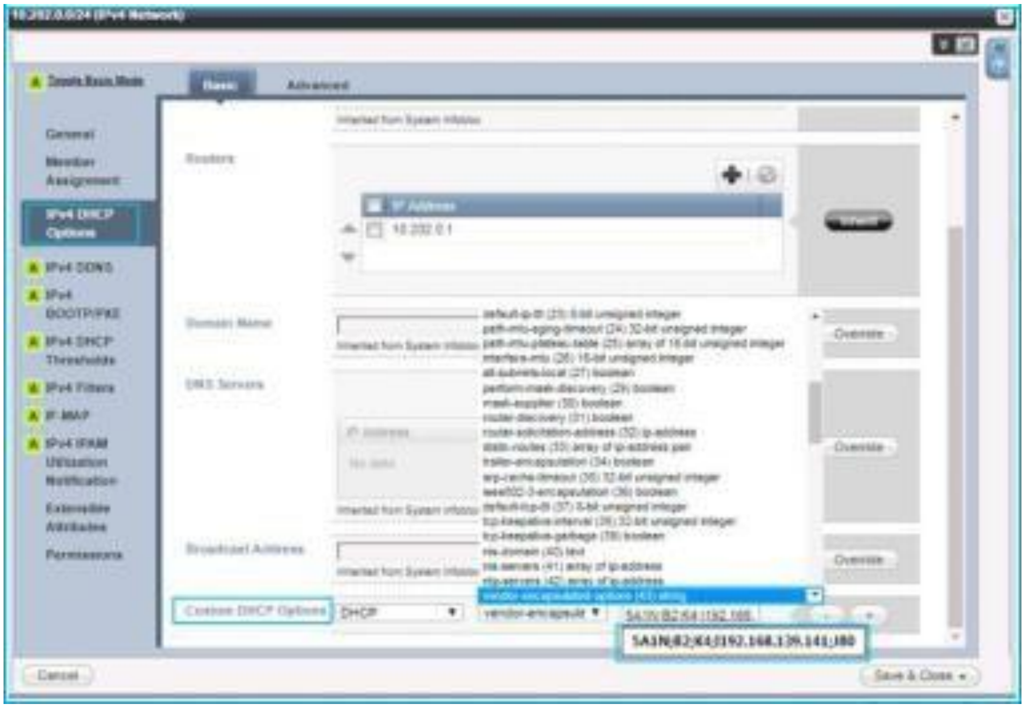


Network	Comment	IPv4 DHCP Util...	Discover Now	Discovery Engine	Site
☑ 10.202.0.0/24	zaf-mgmt	4.0% (2/50)		None	

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;I192.168.139.141;J80.

Step 2: Option 43 Configuration on Infoblox



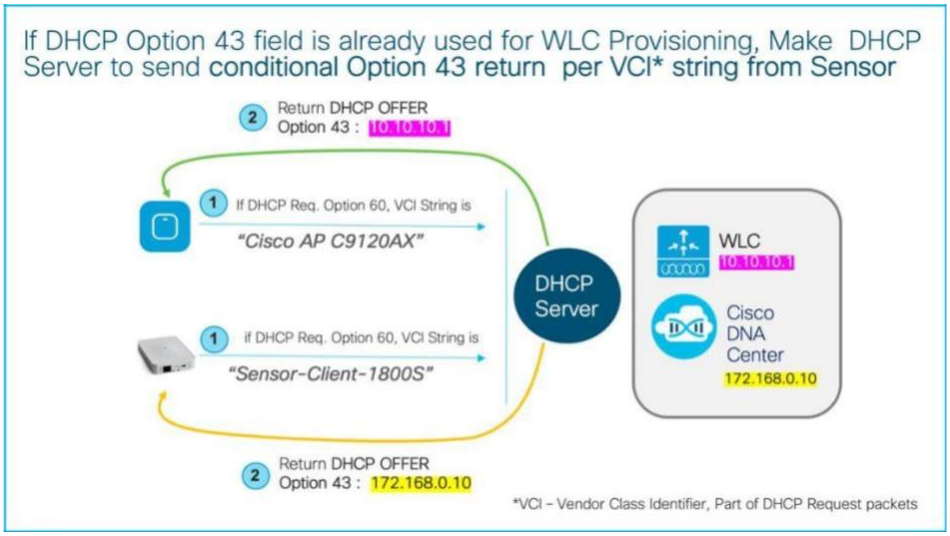
10.202.0.0/24 (IPv4 Network)

Custom DHCP Options: DHCP ▾ vendor-encapsulated-options (43) string

5A1N;B2;K4;I192.168.139.141;J80

Toggle Basic Mode
Basic
Advanced
General
Member Assignment
IPv4 DHCP Options
IPv4 DDNS
IPv4 BOOTP/PXE
IPv4 DHCP Thresholds
IPv4 Filters
IF-MAP
IPv4 IPAM Utilization Notification
Extensible Attributes
Permissions
Routers
IP Address
10.202.0.1
Domain Name
DNS Servers
Broadcast Address
Inherited from System Infoblox
default-ip-ttl (23) 8-bit unsigned integer
path-mtu-aging-timeout (24) 32-bit unsigned integer
path-mtu-plateau-table (25) array of 16-bit unsigned integer
interface-mtu (26) 16-bit unsigned integer
all-subnets-local (27) boolean
perform-mask-discovery (29) boolean
mask-supplier (30) boolean
router-discovery (31) boolean
router-solicitation-address (32) ip-address
static-routes (33) array of ip-address pair
trailer-encapsulation (34) boolean
arp-cache-timeout (35) 32-bit unsigned integer
ieee802-3-encapsulation (36) boolean
default-tcp-ttl (37) 8-bit unsigned integer
tcp-keepalive-interval (38) 32-bit unsigned integer
tcp-keepalive-garbage (39) boolean
nis-domain (40) text
nis-servers (41) array of ip-address
ntp-servers (42) array of ip-address
Override
Cancel
Save & Close

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).



If DHCP Option 43 field is already used for WLC Provisioning, Make DHCP Server to send **conditional Option 43 return per VCI* string from Sensor**

*VCI – Vendor Class Identifier, Part of DHCP Request packets

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.

Disclaimer: If your Cisco DNA Center (version 1.3.3.0 or above) is configured with **only** a domain name, and your Aironet Active Sensor(s) are running an image earlier than 1.3.1.0, follow the steps below to ensure that the sensor's PnP onboarding is successful.

- Create a DNS entry for "data.<FQDN>" (i.e., data.citisvs.cisco.com) and configure the resolution IP to be the same IP as what the "dnac.<FQDN>" the string within your PnP option 43 string (i.e., option 43 ASCII 5A1N;B2;K4;Idnac.citisvs.com;J80) would resolve to.

Note: The above is not applicable if your Cisco DNA Center's certificate's common name contains an IP address.

DNS-Based Cisco DNA Center Discovery

You can create a host record on the DNS server for the domain with the name *PNPSERVER* 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.

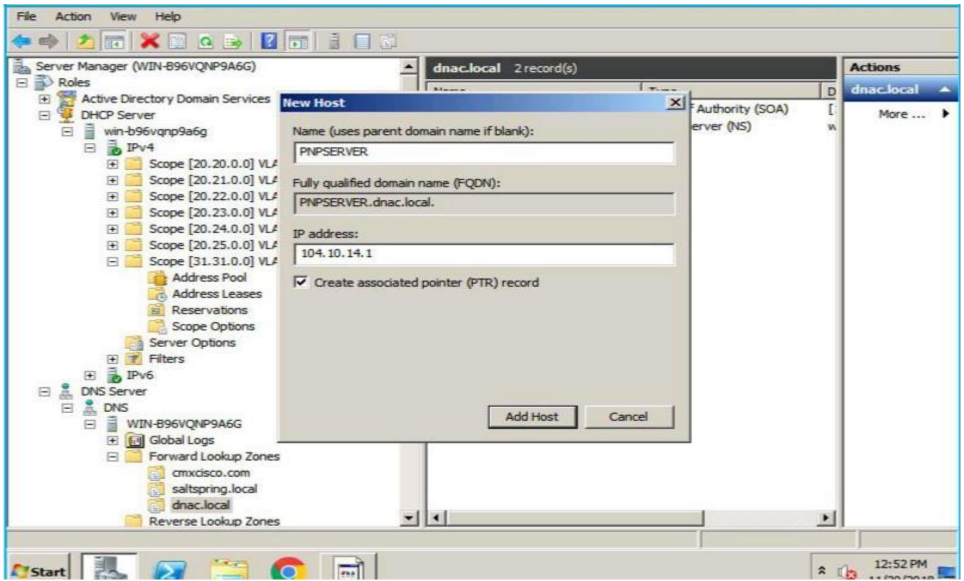
For more information on DNS name-based discovery, see https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Plug-and-Play/solution/guidexml/b_pnp-solution-guide.html#con_115728.

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



New Host

Name (uses parent domain name if blank): PNPSERVER

Fully qualified domain name (FQDN): PNPSERVER.dnac.local.

IP address: 104.10.14.1

☑ Create associated pointer (PTR) record

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:

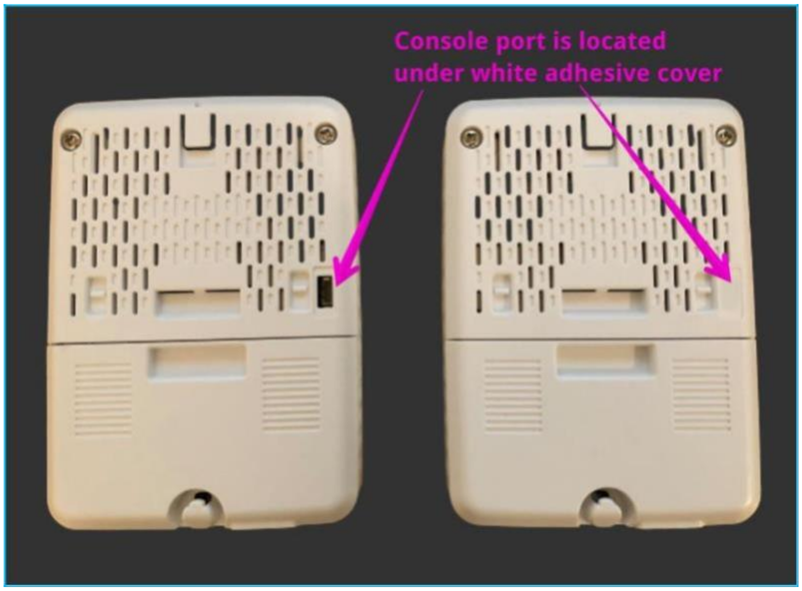
```
#config dot11 sensor pnp ip <ip address of Cisco DNA Center>
```

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.

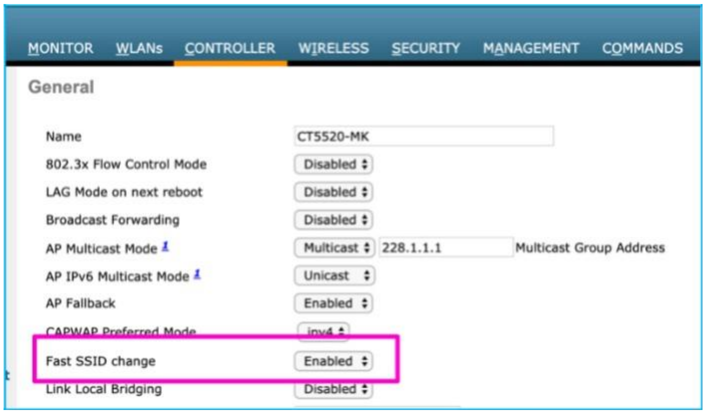
4. Upgrade the sensor image.

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.



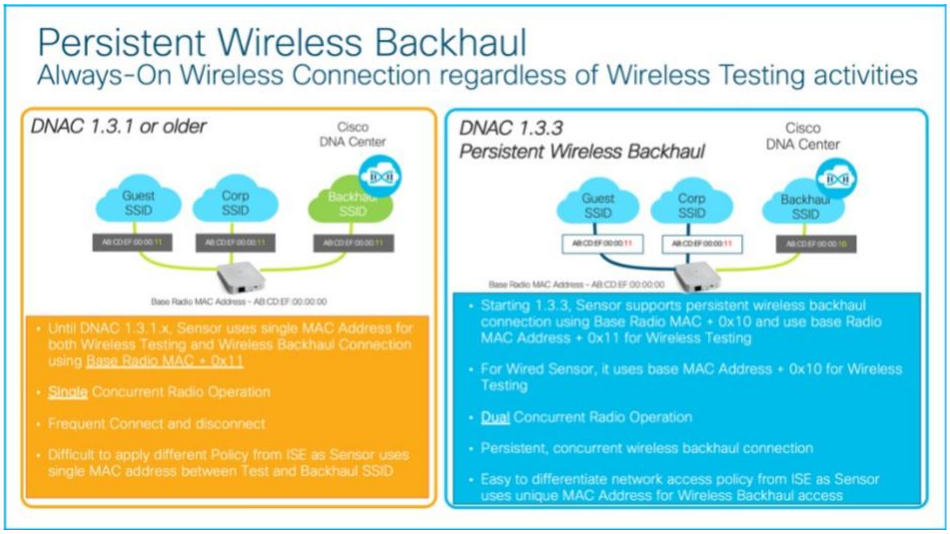
General

Name	CT5520-MK
802.3x Flow Control Mode	Disabled
LAG Mode on next reboot	Disabled
Broadcast Forwarding	Disabled
AP Multicast Mode	Multicast 228.1.1.1 Multicast Group Address
AP IPv6 Multicast Mode	Unicast
AP Fallback	Enabled
CAPWAP Preferred Mode	ipv4
Fast SSID change	Enabled
Link Local Bridging	Disabled

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.



Persistent Wireless Backhaul

Always-On Wireless Connection regardless of Wireless Testing activities

DNAC 1.3.1 or older

- Until DNAC 1.3.1.x, Sensor uses single MAC Address for both Wireless Testing and Wireless Backhaul Connection using Base Radio MAC + 0x11
- Single Concurrent Radio Operation
- Frequent Connect and disconnect
- Difficult to apply different Policy from ISE as Sensor uses single MAC address between Test and Backhaul SSID

DNAC 1.3.3
Persistent Wireless Backhaul

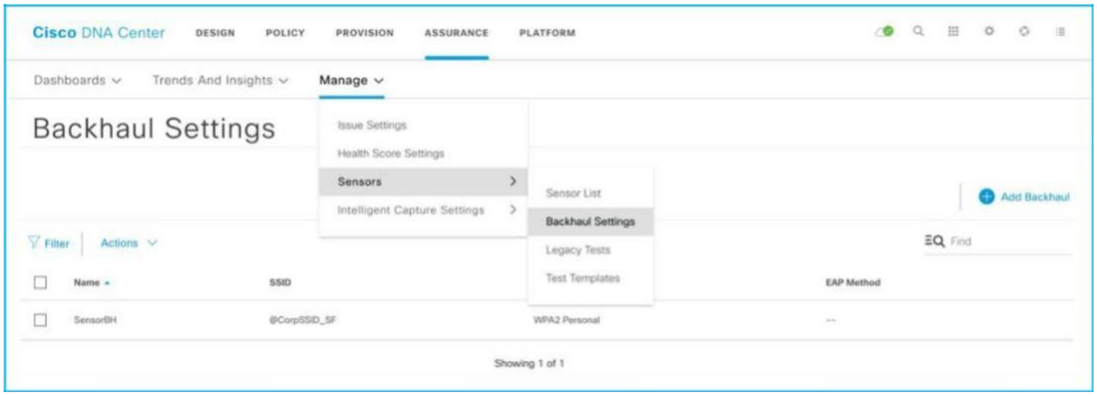
- Starting 1.3.3, Sensor supports persistent wireless backhaul connection using Base Radio MAC + 0x10 and use base Radio MAC Address + 0x11 for Wireless Testing
- For Wired Sensor, it uses base MAC Address + 0x10 for Wireless Testing
- Dual Concurrent Radio Operation
- Persistent, concurrent wireless backhaul connection
- Easy to differentiate network access policy from ISE as Sensor uses unique MAC Address for Wireless Backhaul access

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 *CiscoSensorProvisoning* 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.)



Backhaul Settings

□	Name	SSID		EAP Method
□	SensorBH	@CorpSSID_SF	WPA2 Personal	--

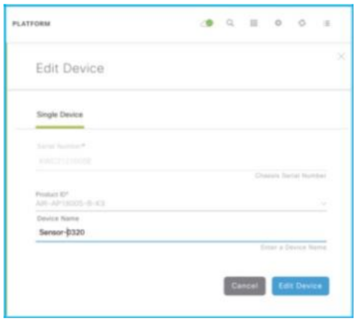
Showing 1 of 1

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.



Edit Device

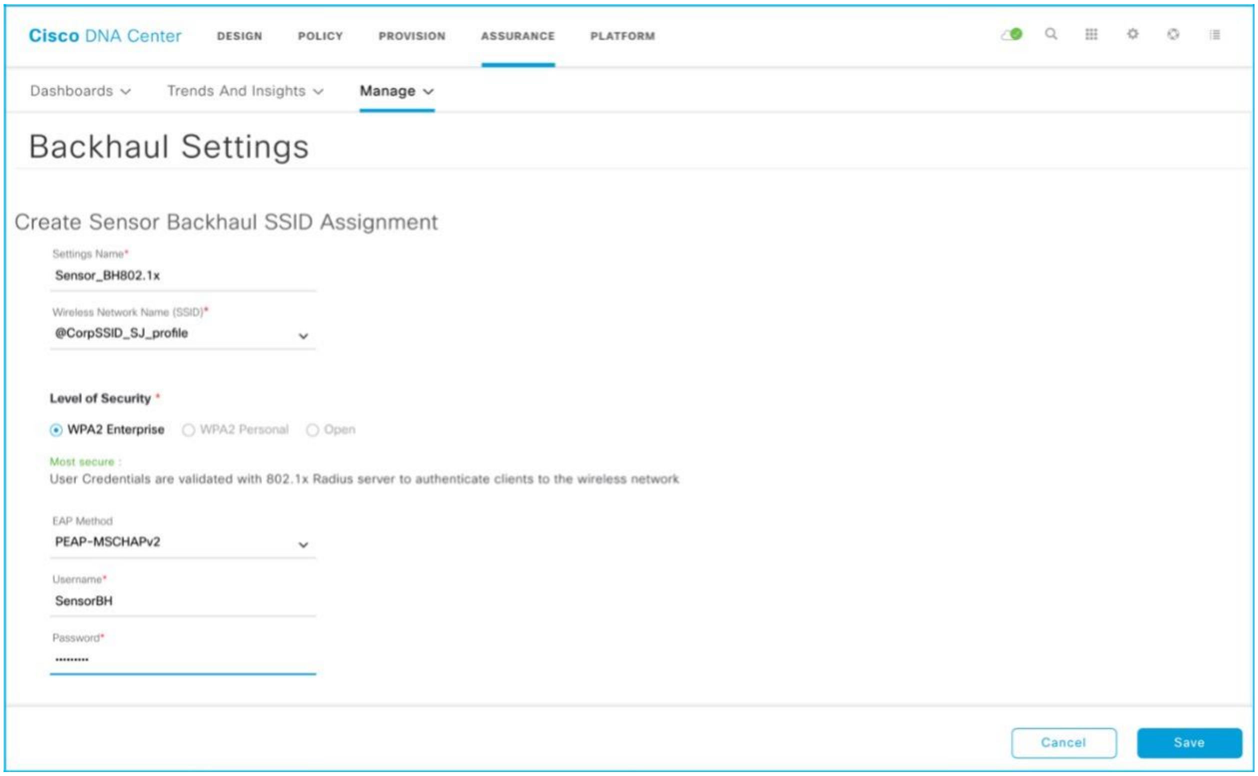
Single Device

Serial Number*
KWC2123000E
Chassis Serial Number

Product ID*
AIR-AP1800S-B-K9

Device Name
Sensor-0320
Enter a Device Name

Sensor Backhaul Settings from Cisco DNA Center



Backhaul Settings

Create Sensor Backhaul SSID Assignment

Settings Name*
Sensor_BH802.1x

Wireless Network Name (SSID)*
@CorpSSID_SJ_profile

Level of Security *
● WPA2 Enterprise ○ WPA2 Personal ○ Open

Most secure :
User Credentials are validated with 802.1x Radius server to authenticate clients to the wireless network

EAP Method
PEAP-MSCHAPv2

Username*
SensorBH

Password*
•••••••••

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.

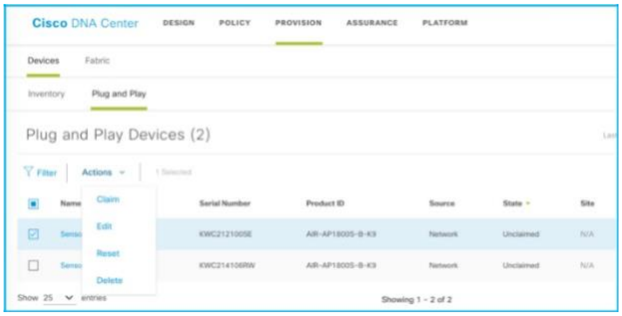
2. If your sensor uses a wireless backhaul connection, power the sensor by plugging it into a wall power socket or use the adapter and attached micro USB-B connector. For either backhaul type, ensure that the sensor has HTTP (TCP 80) and HTTPS (TCP 443) reachability to the Cisco DNA Center server.

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**.

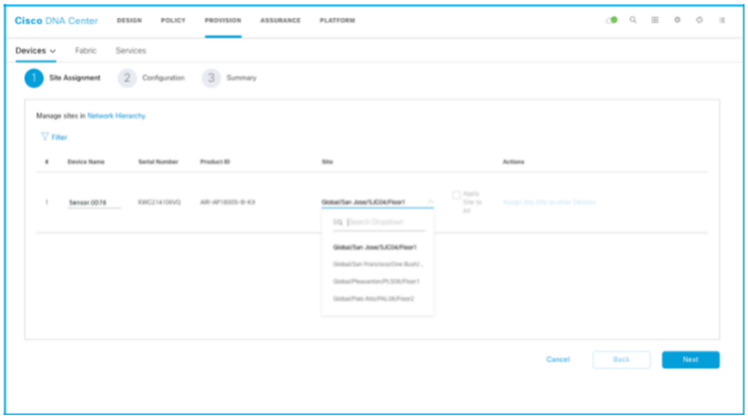


Plug and Play Devices (2)

☐	Name	Serial Number	Product ID	Source	State	Site
☑	Senso	KWC2121005E	AIR-AP1800S-B-K9	Network	Unclaimed	N/A
☐	Senso	KWC214106RW	AIR-AP1800S-B-K9	Network	Unclaimed	N/A

Showing 1 - 2 of 2

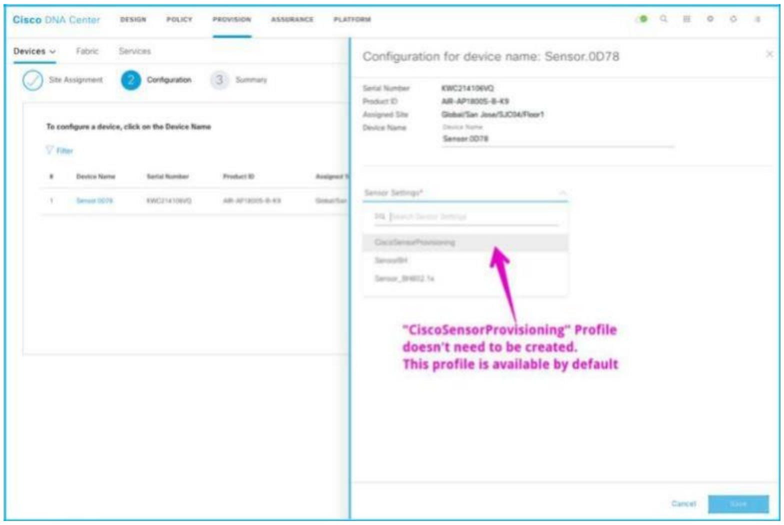
5. After you change the sensor name, your sensor is ready to be provisioned. Select the sensor from the **Unclaimed Device** list and click **Claim Device**.



Manage sites in Network Hierarchy

#	Device Name	Serial Number	Product ID	Site		Actions
1	Sensor.0D78	KWC214106VQ	AIR-AP1800S-B-K9	Global/San Jose/SJC04/Floor1	☐ Apply Site to All	Assign this Site to other Devices

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



To configure a device, click on the Device Name

#	Device Name	Serial Number	Product ID	Assigned S
1	Sensor.0D78	KWC214106VQ	AIR-AP1800S-B-K9	Global/San

Configuration for device name: Sensor.0D78

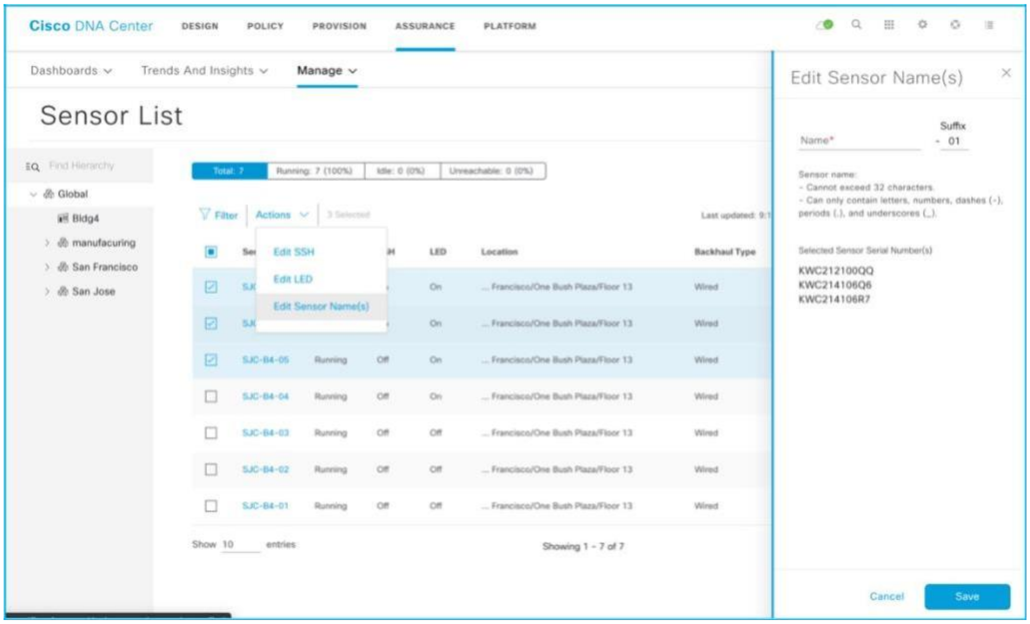
Serial Number KWC214106VQ
Product ID AIR-AP1800S-B-K9
Assigned Site Global/San Jose/SJC04/Floor1
Device Name Sensor.0D78

Sensor Settings*

"CiscoSensorProvisioning" Profile doesn't need to be created.
This profile is available by default

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)**.



Sensor List

Total: 7 | Running: 7 (100%) | Idle: 0 (0%) | Unreachable: 0 (0%)

Last updated: 9:1

■	Se		H	LED	Location	Backhaul Type
☑	SJ			On	... Francisco/One Bush Plaza/Floor 13	Wired
☑	SJ			On	... Francisco/One Bush Plaza/Floor 13	Wired
☑	SJC-B4-05	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-04	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-03	Running	Off	Off	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-02	Running	Off	Off	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-01	Running	Off	Off	... Francisco/One Bush Plaza/Floor 13	Wired

Show 10 entries

Showing 1 - 7 of 7

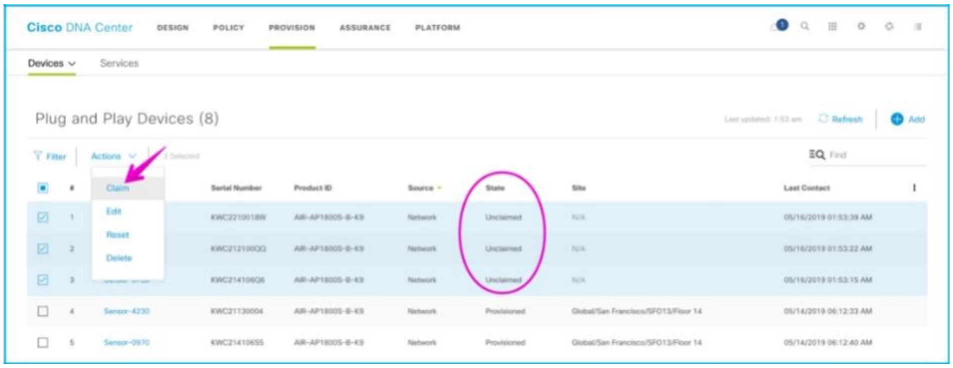
Edit Sensor Name(s)

Name* Suffix - 01

Sensor name:
- Cannot exceed 32 characters.
- Can only contain letters, numbers, dashes (-), periods (.), and underscores (_).

Selected Sensor Serial Number(s)
KWC212100QQ
KWC214106Q6
KWC214106R7

Cisco 1800S Sensor Provisioning – Claiming Device

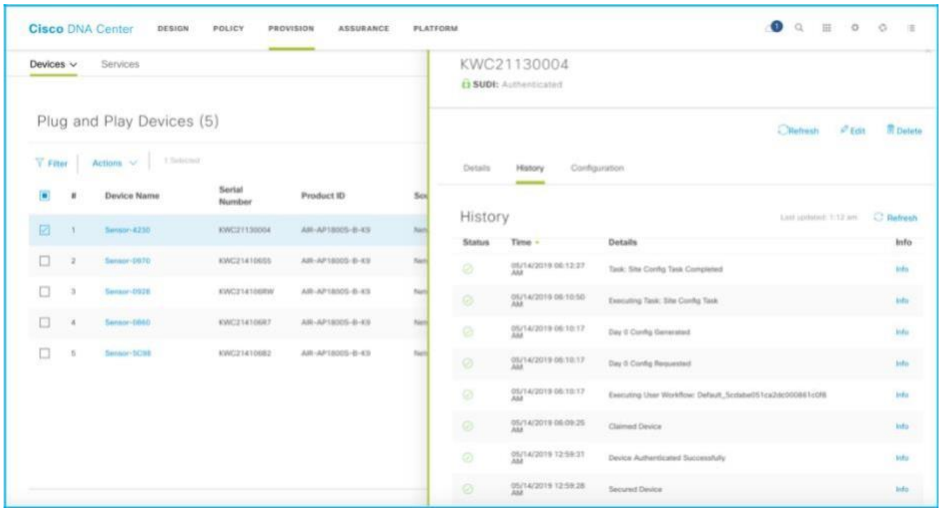


Plug and Play Devices (8)

■	#		Serial Number	Product ID	Source	State	Site	Last Contact
☑	1		KWC2210018W	AIR-AP1800S-B-K9	Network	Unclaimed	N/A	05/16/2019 01:53:39 AM
☑	2		KWC212100QQ	AIR-AP1800S-B-K9	Network	Unclaimed	N/A	05/16/2019 01:53:22 AM
☑	3		KWC214106Q6	AIR-AP1800S-B-K9	Network	Unclaimed	N/A	05/16/2019 01:53:15 AM
□	4	Sensor-4230	KWC21130004	AIR-AP1800S-B-K9	Network	Provisioned	Global/San Francisco/SFO13/Floor 14	05/14/2019 06:12:33 AM
□	5	Sensor-0970	KWC2141065S	AIR-AP1800S-B-K9	Network	Provisioned	Global/San Francisco/SFO13/Floor 14	05/14/2019 06:12:40 AM

The device status changes from **Unclaimed** > **Planned** > **Onboarding** > **Provisioned**. The device remains in the provisioned state, unless it is 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



Plug and Play Devices (5)

☑	#	Device Name	Serial Number	Product ID
☑	1	Sensor-4230	KWC21130004	AIR-AP1800S-B-K9
□	2	Sensor-0970	KWC21410655	AIR-AP1800S-B-K9
□	3	Sensor-0928	KWC214106RW	AIR-AP1800S-B-K9
□	4	Sensor-0860	KWC214106R7	AIR-AP1800S-B-K9
□	5	Sensor-5C98	KWC21410682	AIR-AP1800S-B-K9

KWC21130004
SUDI: Authenticated

History

Last updated: 1:12 am

Status	Time	Details	Info
✓	05/14/2019 06:12:27 AM	Task: Site Config Task Completed	Info
✓	05/14/2019 06:10:50 AM	Executing Task: Site Config Task	Info
✓	05/14/2019 06:10:17 AM	Day 0 Config Generated	Info
✓	05/14/2019 06:10:17 AM	Day 0 Config Requested	Info
✓	05/14/2019 06:10:17 AM	Executing User Workflow: Default_5cdabe051ca2dc000861c0f8	Info
✓	05/14/2019 06:09:25 AM	Claimed Device	Info
✓	05/14/2019 12:59:31 AM	Device Authenticated Successfully	Info
✓	05/14/2019 12:59:28 AM	Secured Device	Info

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.

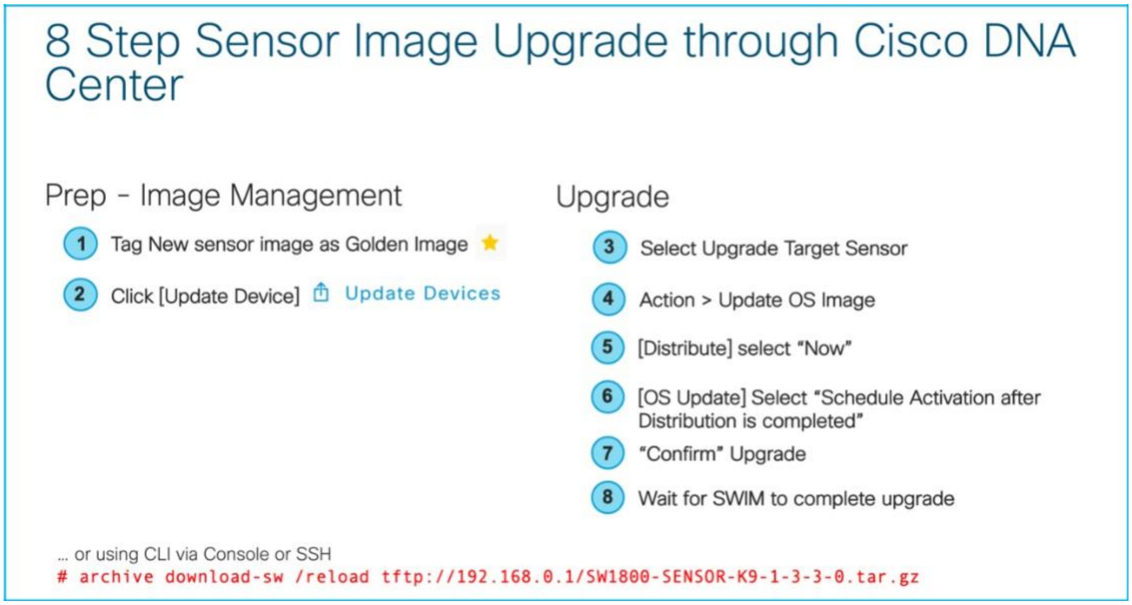
Disclaimer: If your Sensor is running version 8.8.259.0, it only supports using the CiscoSensorProvisioning SSID as a means to contact Cisco DNA Center through Plug and Play, but not as a wireless backhaul method for continued management. To use the CiscoSensorProvisoning SSID as a wireless backhaul method, the network admin needs to upgrade the Sensor software from 8.8.259.0 to 1.3.3.0 or later release. Please follow the steps below to claim your 8.8.259.0 sensor to Cisco DNA Center properly:

1. Create a custom wireless backhaul profile.
2. Claim the Sensor from the PnP page to the custom wireless backhaul profile created.

If you'd like your sensors to use the CiscoSensorProvisioning SSID as the wireless backhaul, continue with the following steps:

1. Upgrade the Sensor to 1.3.3.0 or above through the image repository page described in "Upgrade Sensor Section" below.
2. Delete your claimed Sensor from inventory, and it will show up on the Plug and Play page as unclaimed again.
3. Claim the Sensor again, but this time to the CiscoSensorProvisioning backhaul profile.

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
```

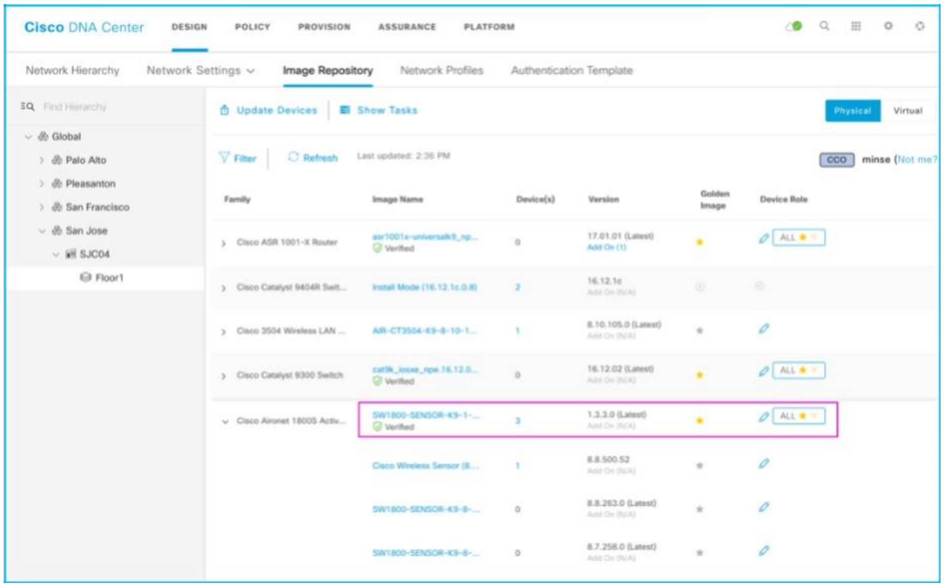
Provision Sensors

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.

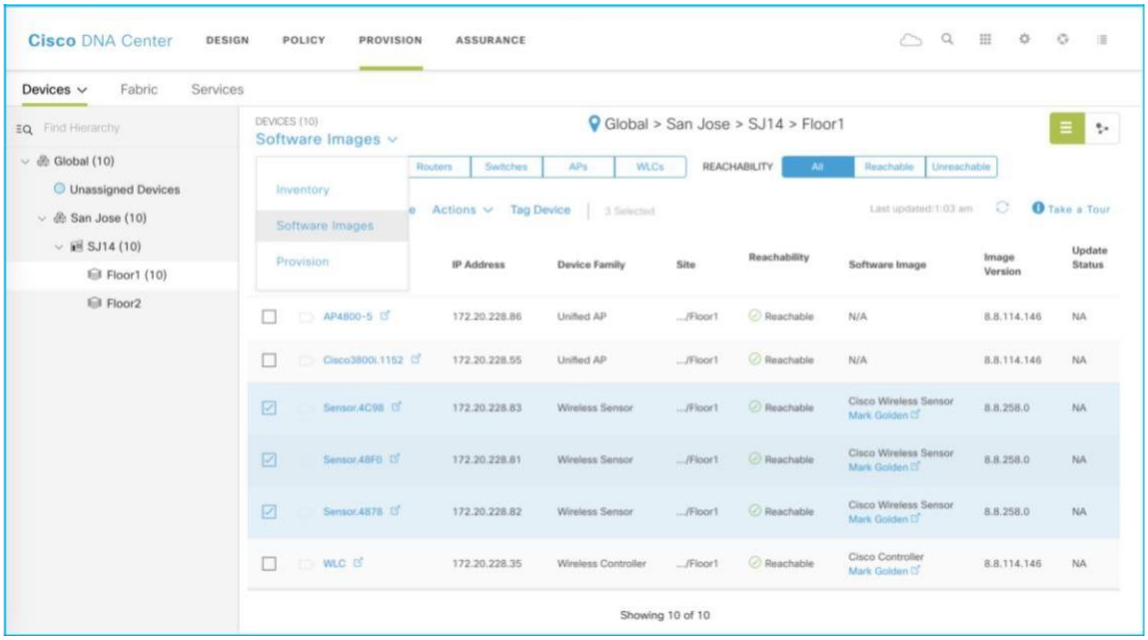
Alternatively, you can manually import the sensor software into Cisco DNA Center from your local browser. Import the sensor software from the Image Repository tool, which is integrated as part of Design option in Cisco DNA Center 1.3, by clicking **Design > Image Repository**.



	Family	Image Name	Device(s)	Version	Golden Image	Device Role
›	Cisco ASR 1001-X Router	asr1001x-universalk9_np... ✓ Verified	0	17.01.01 (Latest) Add On (1)	★	ALL ★
›	Cisco Catalyst 9404R Swit...	Install Mode (16.12.1c.0.8)	2	16.12.1c Add On (N/A)		
›	Cisco 3504 Wireless LAN ...	AIR-CT3504-K9-8-10-1...	1	8.10.105.0 (Latest) Add On (N/A)	★	
›	Cisco Catalyst 9300 Switch	cat9k_iosxe_npe.16.12.0... ✓ Verified	0	16.12.02 (Latest) Add On (N/A)	★	ALL ★
⌄	Cisco Aironet 1800S Activ...	SW1800-SENSOR-K9-1-... ✓ Verified	3	1.3.3.0 (Latest) Add On (N/A)	★	ALL ★
		Cisco Wireless Sensor (8....	1	8.8.500.52 Add On (N/A)	★	
		SW1800-SENSOR-K9-8-...	0	8.8.263.0 (Latest) Add On (N/A)	★	
		SW1800-SENSOR-K9-8-...	0	8.7.258.0 (Latest) Add On (N/A)	★	

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.

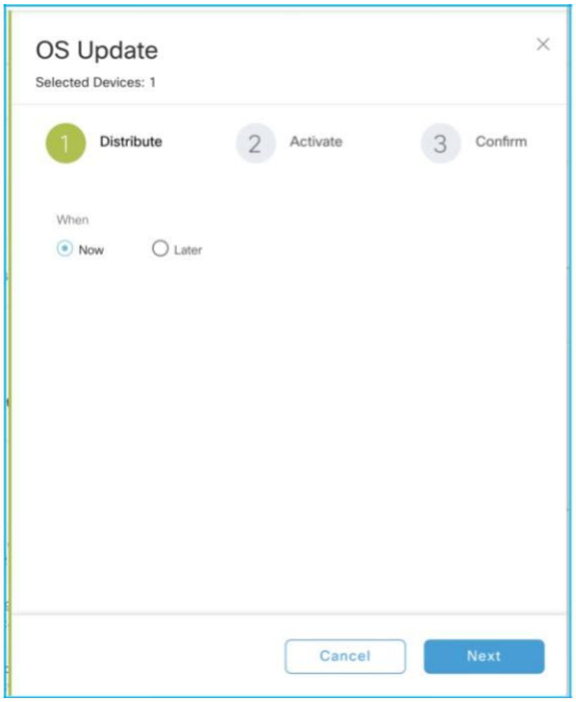


		IP Address	Device Family	Site	Reachability	Software Image	Image Version	Update Status
☐	AP4800-5	172.20.228.86	Unified AP	.../Floor1	Reachable	N/A	8.8.114.146	NA
☐	Cisco3800I.1152	172.20.228.55	Unified AP	.../Floor1	Reachable	N/A	8.8.114.146	NA
☑	Sensor.4C98	172.20.228.83	Wireless Sensor	.../Floor1	Reachable	Cisco Wireless Sensor Mark Golden	8.8.258.0	NA
☑	Sensor.48F0	172.20.228.81	Wireless Sensor	.../Floor1	Reachable	Cisco Wireless Sensor Mark Golden	8.8.258.0	NA
☑	Sensor.4878	172.20.228.82	Wireless Sensor	.../Floor1	Reachable	Cisco Wireless Sensor Mark Golden	8.8.258.0	NA
☐	WLC	172.20.228.35	Wireless Controller	.../Floor1	Reachable	Cisco Controller Mark Golden	8.8.114.146	NA

Showing 10 of 10

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.

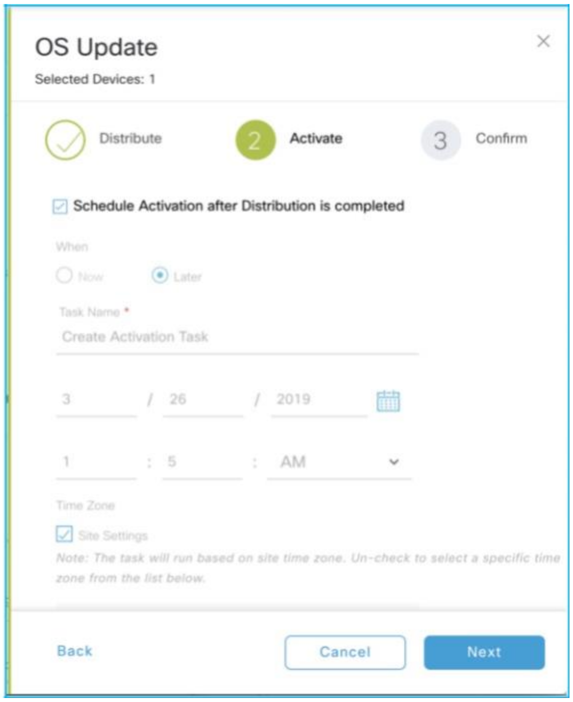


OS Update

Selected Devices: 1

When

● Now ○ Later



OS Update

Selected Devices: 1

☑ Schedule Activation after Distribution is completed

When

○ Now ● Later

Task Name *

Create Activation Task

3 / 26 / 2019

1 : 5 : AM

Time Zone

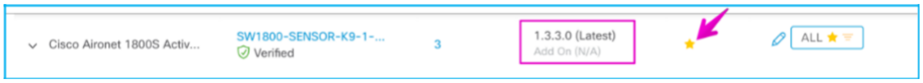
☑ Site Settings

Note: The task will run based on site time zone. Un-check to select a specific time zone from the list below.

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.



Cisco Aironet 1800S Activ...	SW1800-SENSOR-K9-1-... Verified	3	1.3.3.0 (Latest) Add On (N/A)	★

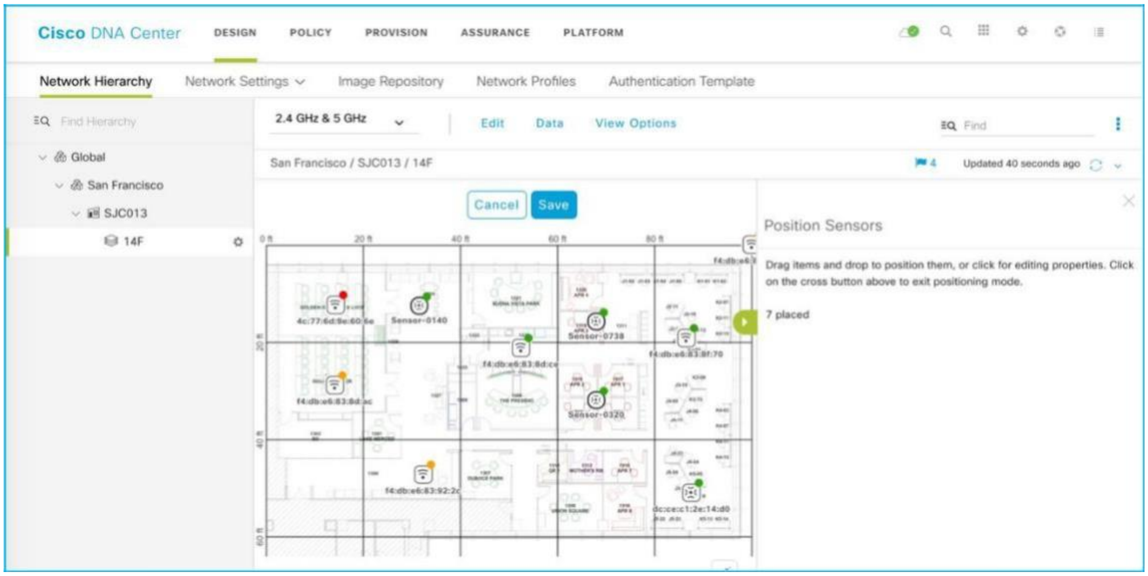
- The sensor is in a partial collection failure status. This status means that the sensor failed to exchange heartbeats with Cisco DNA Center. In this case, the image upgrade is not initiated. Only after all of the selected sensors are ready to be upgraded can select **Now** to start the upgrade of all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



Position Sensors

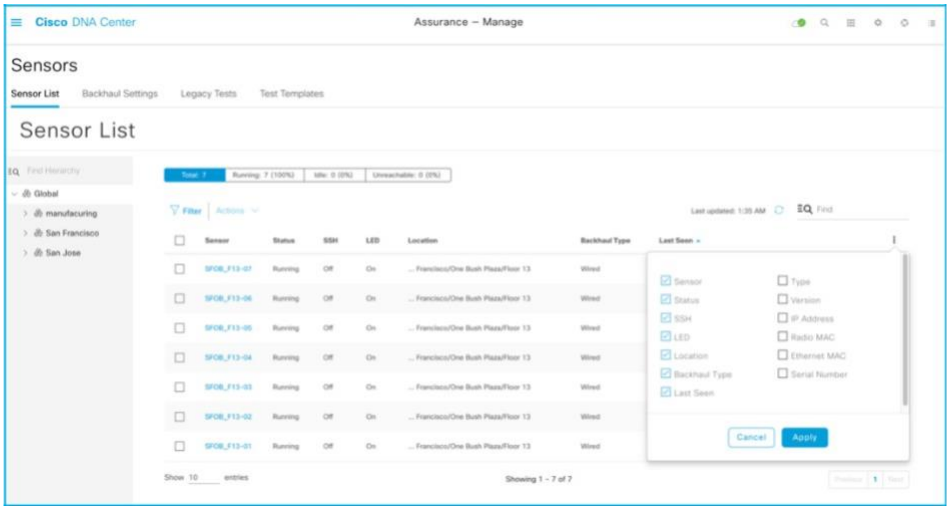
Drag items and drop to position them, or click for editing properties. Click on the cross button above to exit positioning mode.

7 placed

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



Sensor List

□	Sensor	Status	SSH	LED	Location	Backhaul Type	Last Seen
□	SFOB_F13-07	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired	
□	SFOB_F13-06	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired	
□	SFOB_F13-05	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired	
□	SFOB_F13-04	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired	
□	SFOB_F13-03	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired	
□	SFOB_F13-02	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired	
□	SFOB_F13-01	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired	

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**.

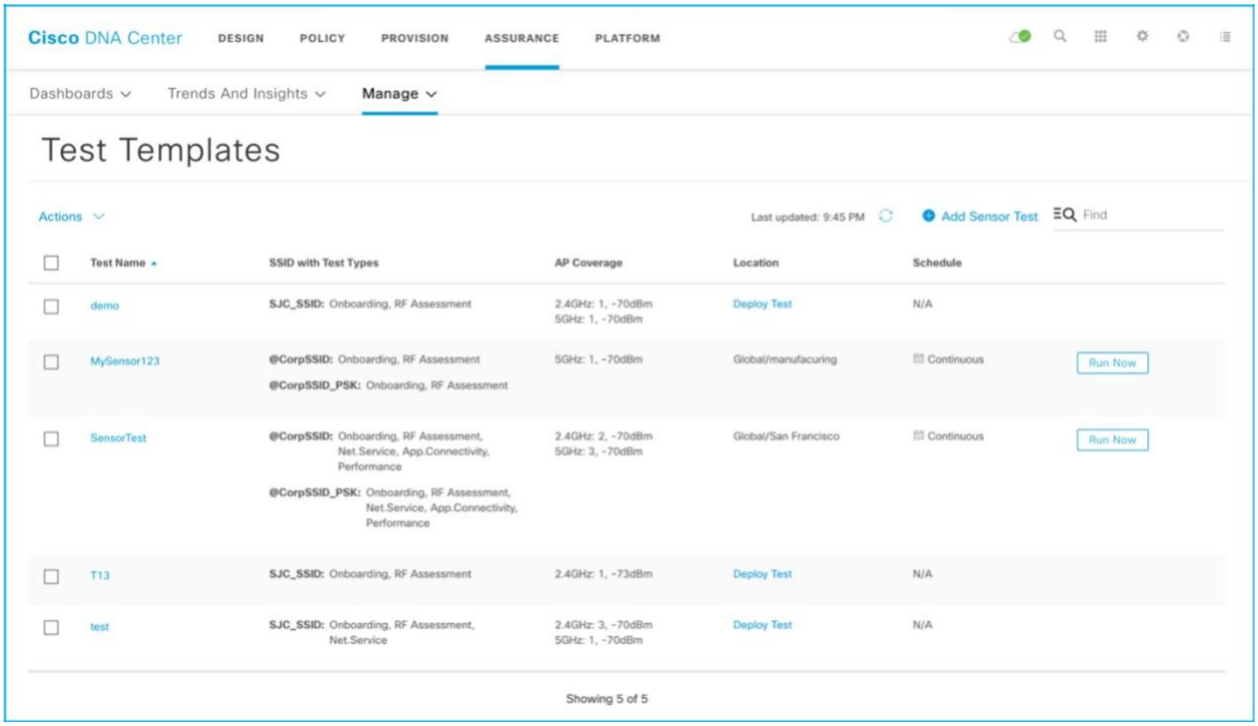
Note: A sensor uses a single admin ID between SSH and CLI, so if you change the username and password of a sensor, both the SSH and CLI login credential are changed.

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 Templates

Last updated: 9:45 PM

□	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/manufacuring	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.

Onboarding

- **Association, Authentication, DHCP**
  - **Description:** The sensor attempts to join the user-defined wireless network.
  - **Pass Criteria:** The sensor can join the wireless network and receive an IP address.

RF Assessment

- **Data Rate, SNR**
  - **Description:** The sensor attempts to collect data rates and SNR data from non-onboarding tests.
  - **Pass Criteria:** The sensor can collect data rates and SNR data from non-onboarding tests.
  - **Note:** RF assessment tests are not run unless additional non-onboarding tests, such as DNS, RADIUS, and so on, are configured.

Network Services Tests

- **DNS**
  - **Description:** The sensor attempts to resolve the user-defined hostname through the network's DNS server.
  - **Pass Criteria:** The sensor can reach the network's DNS server and resolve the hostname.

- **RADIUS – Authenticating Client (Part 1)**
  - **Prerequisite:** Create a user identity entry within the network's RADIUS server, which includes a user-defined username and password.
  - **Description:** The sensor acts as a client and attempts to authenticate into the 802.1x enterprise security network using the user-defined username and password.
  - **Pass Criteria:** The sensor can authenticate itself into the wireless network as a client.

- **RADIUS – Client Authenticator (Part 2)**
  - **Prerequisite:** Create a client authenticator entry within the network's RADIUS server, which includes the sensor's IP address and a user-defined shared secret.
  - **Description:** The sensor acts as the client authenticator and attempts to connect to the network's RADIUS server using the user-defined shared secret, port number, and protocol (PAP or CHAP).
  - **Pass Criteria:** The sensor can establish communication with the RADIUS server as a client authenticator.
  - **Note:** If only the active user directory is used to authenticate, only PAP is supported

Performance Tests

- **Internet (NDT)**
  - **Description:** The sensor attempts to run a performance test to the nearest public or user-defined private MLAB server to obtain downlink and uplink throughput data as well as latency through port 3001.
  - **Pass Criteria:** The sensor can reach the MLAB server and collect throughput, latency, and packet loss data.

- **iPerf3**
  - **Description:** The sensor attempts to run a performance test to the user-defined private iPerf3 server.
  - **Pass Criteria:** The sensor can reach the iPerf3 server and collect throughput, latency, and packet loss data.

- **IP SLA**
  - **Description:** The sensor attempts to send a UDP probe to the wireless network using the user-defined traffic service level (Platinum, Gold, Silver, Bronze) and function as the responder to determine the jitter, latency, packet loss, and round-trip time of the last hop.
  - **Pass Criteria:** The sensor can reach the wireless network and collect latency, packet loss, jitter, and round-trip time data.
  - **Note:** IP SLA Testing is not supported in the following conditions:
    - The Cisco wireless infrastructure is running Cisco AireOS 8.5 software version.
    - P2P Blocking on your WLAN is enabled.
    - Cisco IOS Wave 1 Series APs.

Application Tests

- **Host Reachability**

  - **Description:** The sensor attempts to reach the user-defined IP address through ping.
  - **Pass Criteria:** The sensor can reach the user-defined IP address through ping.

- **Web**
  - **Description:** The sensor attempts to resolve the user-defined URL through the network's DNS server, and then tries to reach the resolution IP address through port 80 (HTTP) or 443 (HTTPS).
  - **Pass Criteria:** The sensor can reach the network's DNS server, resolve the hostname, reach the resolution IP address, and collect latency and response time data.
- **FTP**
  - **Description:** The sensor attempts to log in to a user-defined FTP server.
    - If you choose the **Upload** option, the sensor uploads the text file to the user-defined path.
    - If you choose the **Download** option, the sensor downloads the file from the user-defined file path.
  - **Pass Criteria:** The sensor can reach the FTP server and either upload and/or download the file successfully.

Application Tests

- **POP3**
  - **Description:** The sensor attempts to reach the user-defined POP3 server through port 110.
  - **Pass Criteria:** The sensor can reach the POP3 server through port 110.

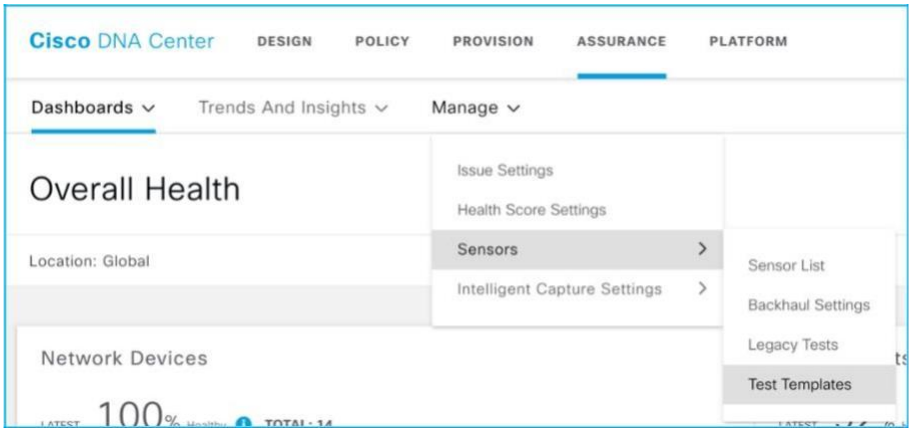
- **IMAP**
  - **Description:** The sensor attempts to reach the user-defined IMAP server through port 143.
  - **Pass Criteria:** The sensor can reach the IMAP server through port 143.

- **Outlook Web Access**
  - **Description:** The sensor attempts to log in and log out of the user-defined Outlook Web Access server (**Example:** https://owa.example.com).
  - **Pass Criteria:** The sensor can log in and log out of the Outlook Web Access server.

Procedure

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

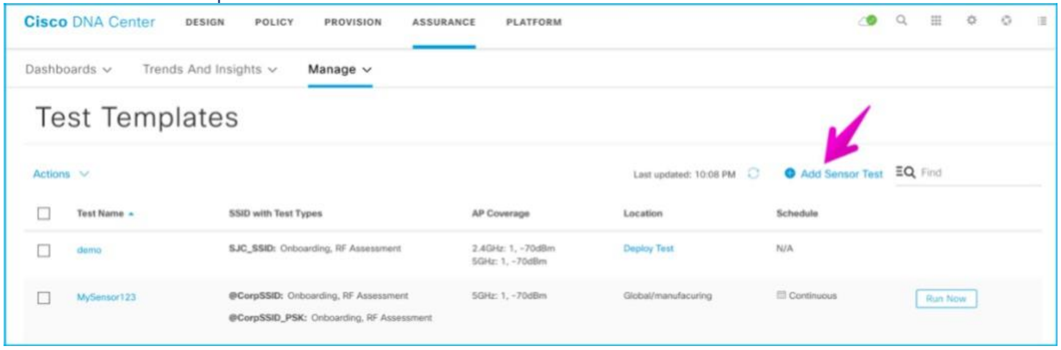
Sensor Tests Templates - Navigation



2. Click **Add Sensor Test**.

Add Sensor Test

Create a Sensor Test Template



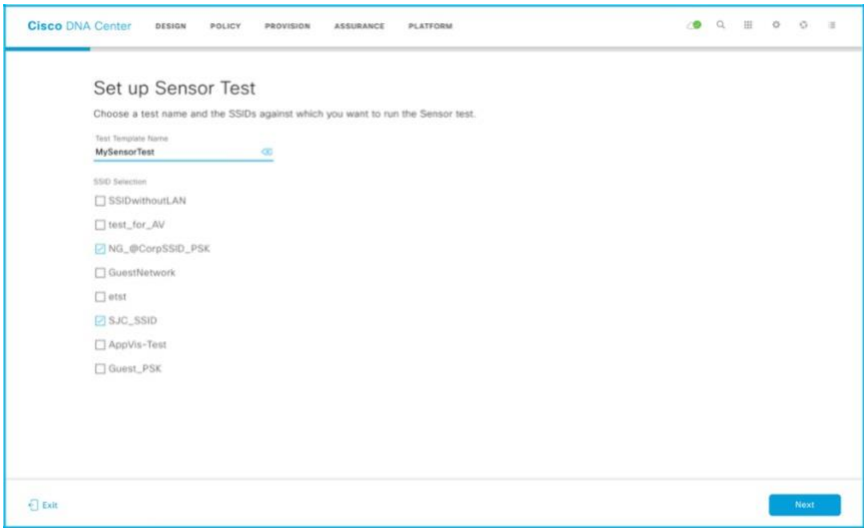
Test Templates

Last updated: 10:08 PM

	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/manufacuring	Continuous	Run Now

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

Set Up Sensor Test



Set up Sensor Test

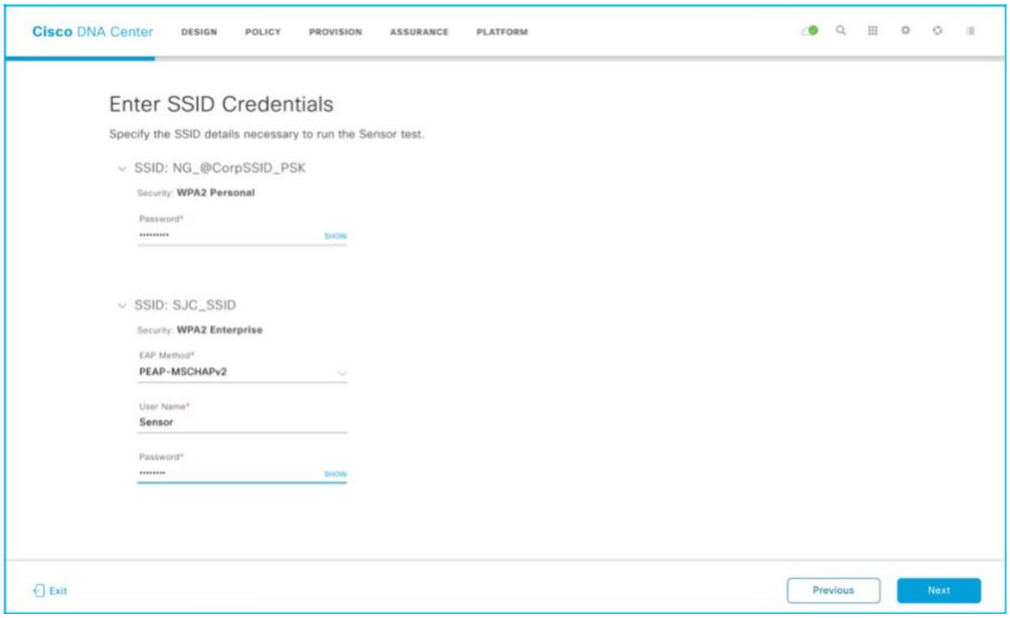
Choose a test name and the SSIDs against which you want to run the Sensor test.

Test Template Name: MySensorTest

SSID Selection

- □ SSIDwithoutLAN
- □ test_for_AV
- ☑ NG_@CorpSSID_PSK
- □ GuestNetwork
- □ etst
- ☑ SJC_SSID
- □ AppVis-Test
- □ Guest_PSK

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



Enter SSID Credentials

Specify the SSID details necessary to run the Sensor test.

SSID: NG_@CorpSSID_PSK

Security: **WPA2 Personal**

Password*: •••••••••

SSID: SJC_SSID

Security: **WPA2 Enterprise**

EAP Method*: PEAP-MSCHAPv2

User Name*: Sensor

Password*: ••••••••

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:

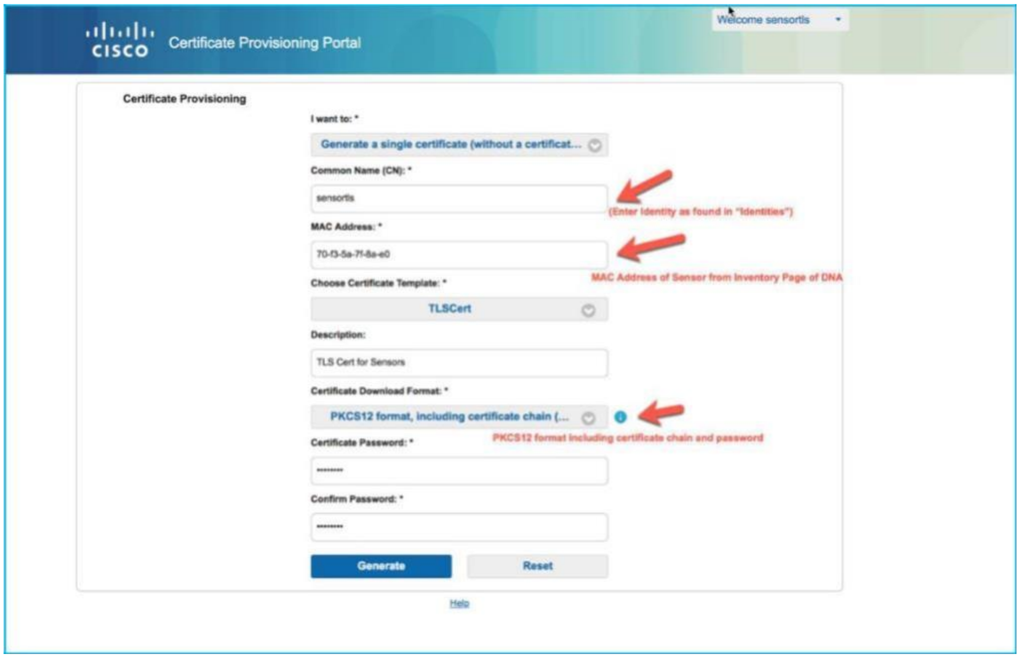
Note: Refer to the following document to setup the certificate provisioning portal in ISE and to generate certificates: https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/200534-ISE-2-0-Certificate-Provisioning-Portal.html

— 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



Certificate Provisioning

I want to: *
Generate a single certificate (without a certificat...

Common Name (CN): *
sensortls

(Enter Identity as found in "Identities")

MAC Address: *
70-f3-5a-7f-8a-e0

MAC Address of Sensor from Inventory Page of DNA

Choose Certificate Template: *
TLSCert

Description:
TLS Cert for Sensors

Certificate Download Format: *
PKCS12 format, including certificate chain (...

PKCS12 format including certificate chain and password

Certificate Password: *
****

Confirm Password: *
****

WebAuth Enabled SSIDs

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

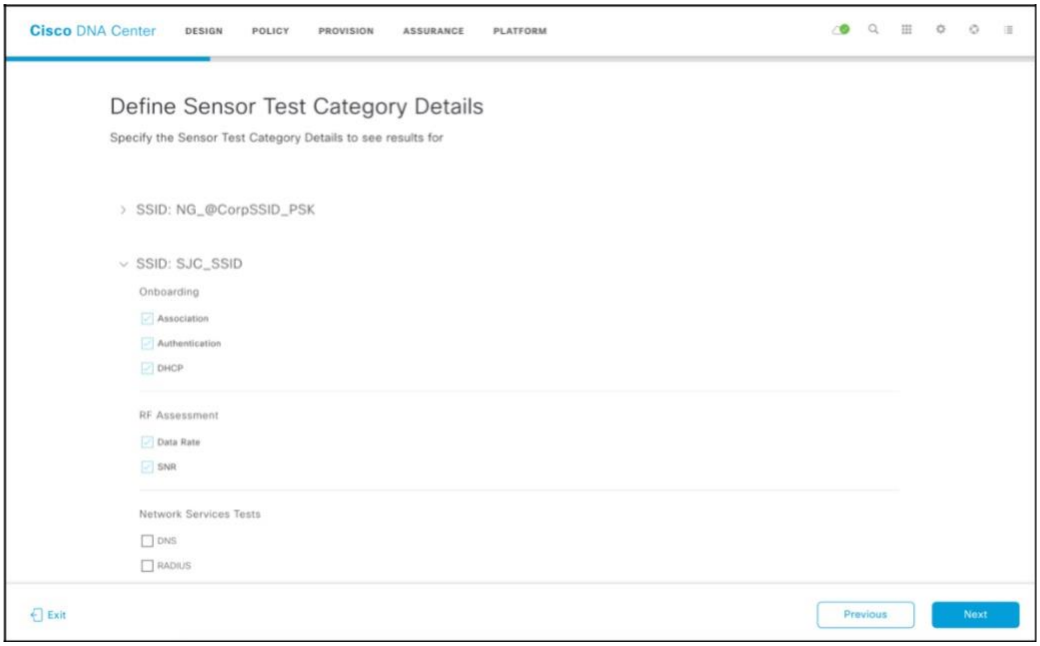
— For WebAuth with user authentication, provide the necessary credentials.

— 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



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

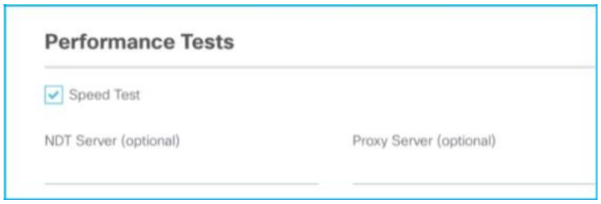
☑ SNR

Network Services Tests

□ DNS

□ RADIUS

Performance Tests – Speed Test



Performance Tests

☑ Speed Test

NDT Server (optional)

Proxy Server (optional)

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:

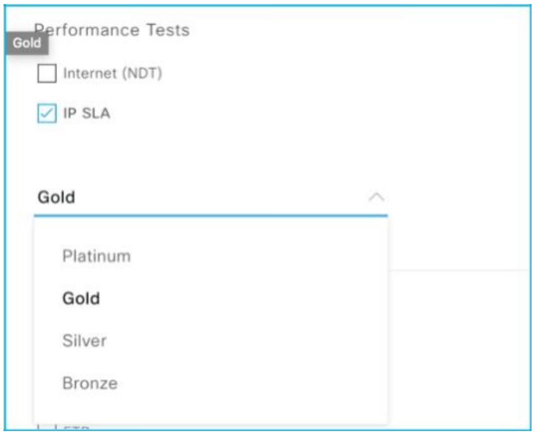
{"city": "San Francisco Bay Area_CA", "url": "http://ndt.iupui.mlab2.nuq07.measurement-lab.org:7123", "ip": ["209.170.110.216", "2001:2030:0:12::216"], "fqdn": "ndt.iupui.mlab2.nuq07.measurement-lab.org", "site": "nuq07", "country": "US"}

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

Gold

□ 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.

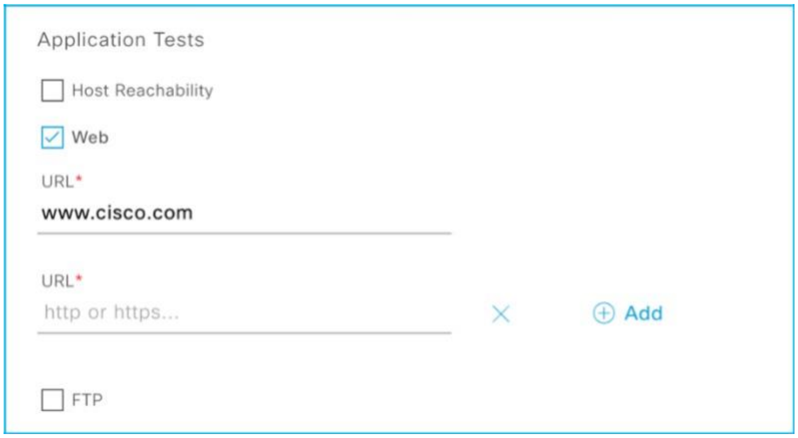
IP SLA testing is supported on Wave-2 (AP1800/2800/3800/4800 series AP) and Wi-Fi 6 APs (Catalyst 9100 series) models running software release 8.8.111 or 16.12.1s.

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...

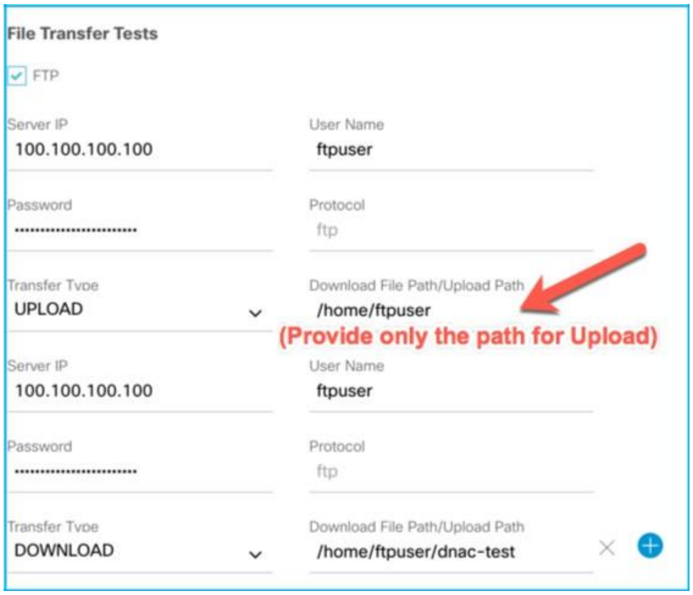
× ⊕ Add

□ FTP

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

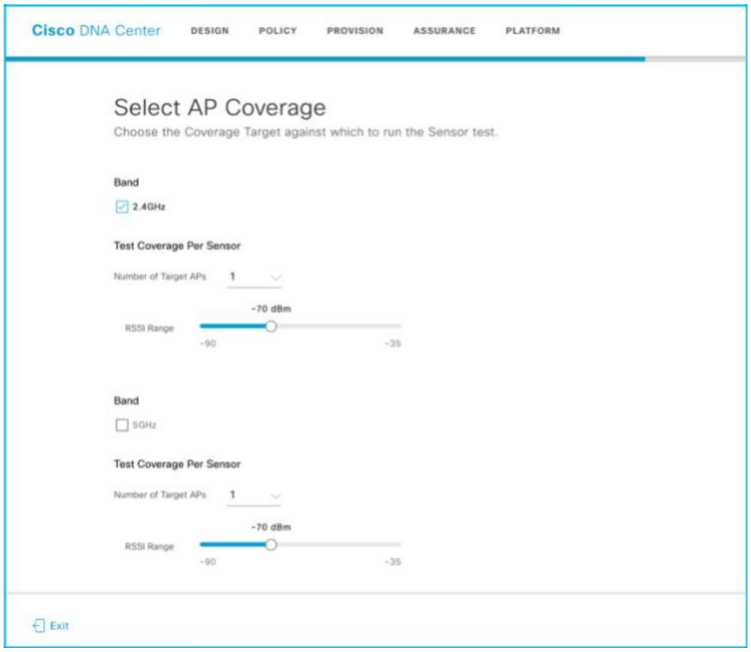
Server IP: 100.100.100.100
User Name: ftpuser
Password: ••••••••••••••••••••••••
Protocol: ftp
Transfer Tvpe: UPLOAD
Download File Path/Upload Path: /home/ftpuser

(Provide only the path for Upload)

Server IP: 100.100.100.100
User Name: ftpuser
Password: ••••••••••••••••••••••••
Protocol: ftp
Transfer Tvpe: DOWNLOAD
Download File Path/Upload Path: /home/ftpuser/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.



Select AP Coverage

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

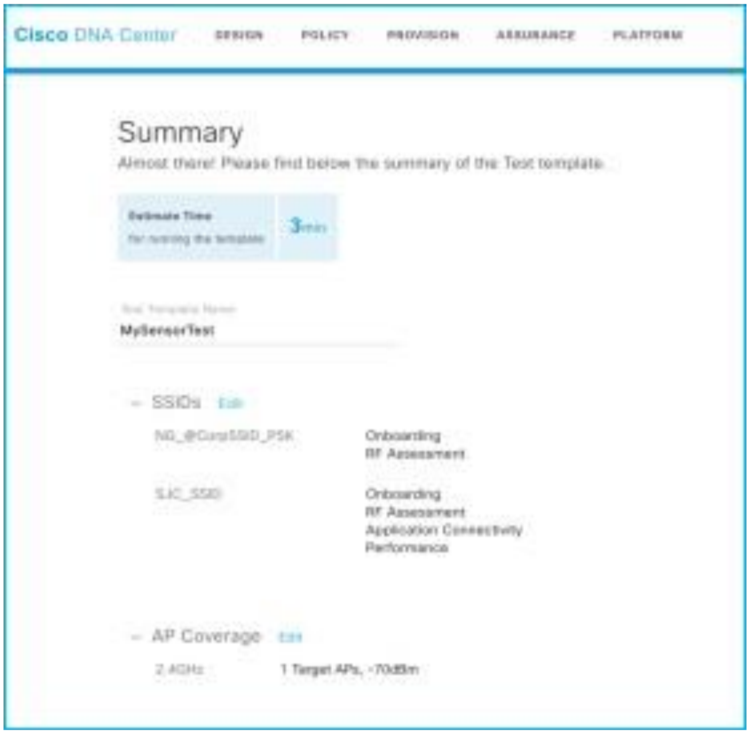
Band
☑ 2.4GHz

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

Band
□ 5GHz

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

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



Summary

Almost there! Please find below the summary of the Test template

Estimate Time
for running the template
3min

Test Template Name
MySensorTest

– SSIDs Edit

NG_@CorpSSID_PSK
Onboarding
RF Assessment

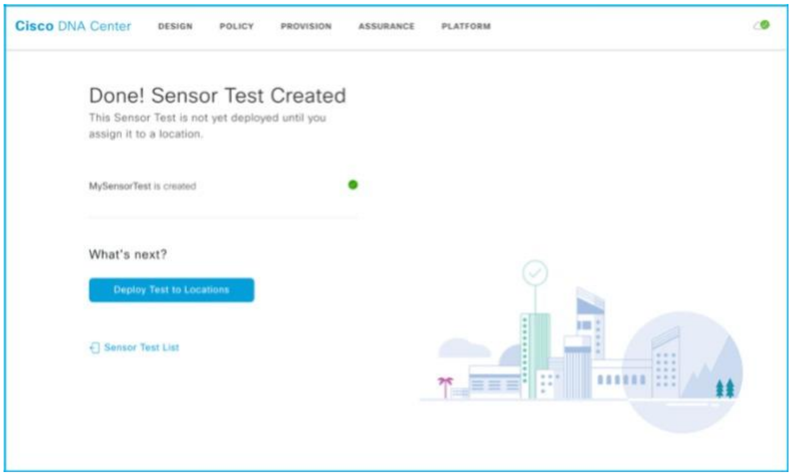
SJC_SSID
Onboarding
RF Assessment
Application Connectivity
Performance

– AP Coverage Edit

2.4GHz
1 Target APs, -70dBm

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.



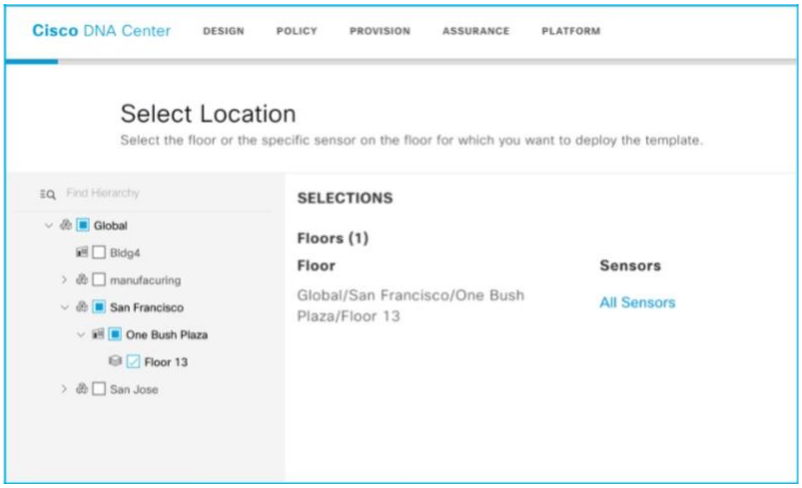
Done! Sensor Test Created

This Sensor Test is not yet deployed until you assign it to a location.

MySensorTest is created ●

What's next?

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



Select Location

Select the floor or the specific sensor on the floor for which you want to deploy the template.

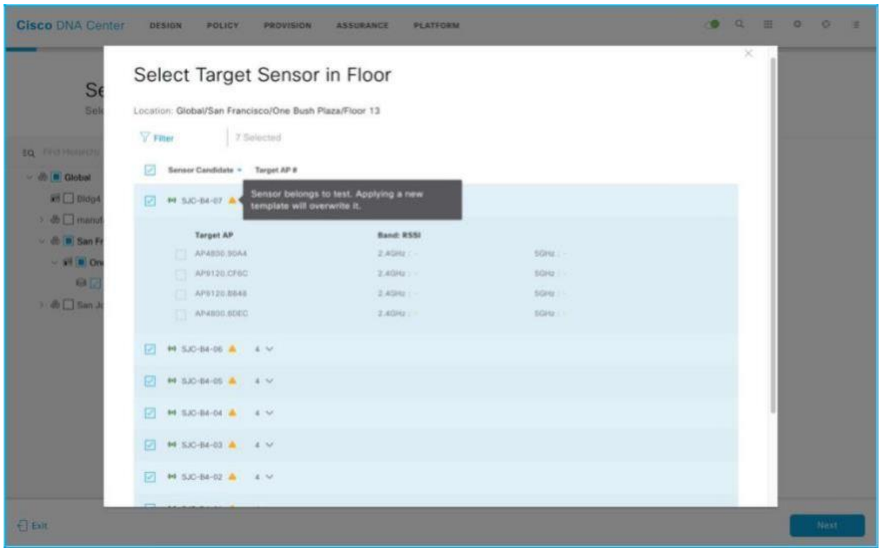
- ■ Global
  - □ Bldg4
  - □ manufacuring
  - ■ San Francisco
    - ■ One Bush Plaza
      - ☑ Floor 13
  - □ San Jose

SELECTIONS

Floors (1)

Floor	Sensors
Global/San Francisco/One Bush Plaza/Floor 13	All Sensors

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.



Select Target Sensor in Floor

Location: Global/San Francisco/One Bush Plaza/Floor 13

7 Selected

☑ Sensor Candidate	Target AP #
☑ SJC-B4-07 ⚠	

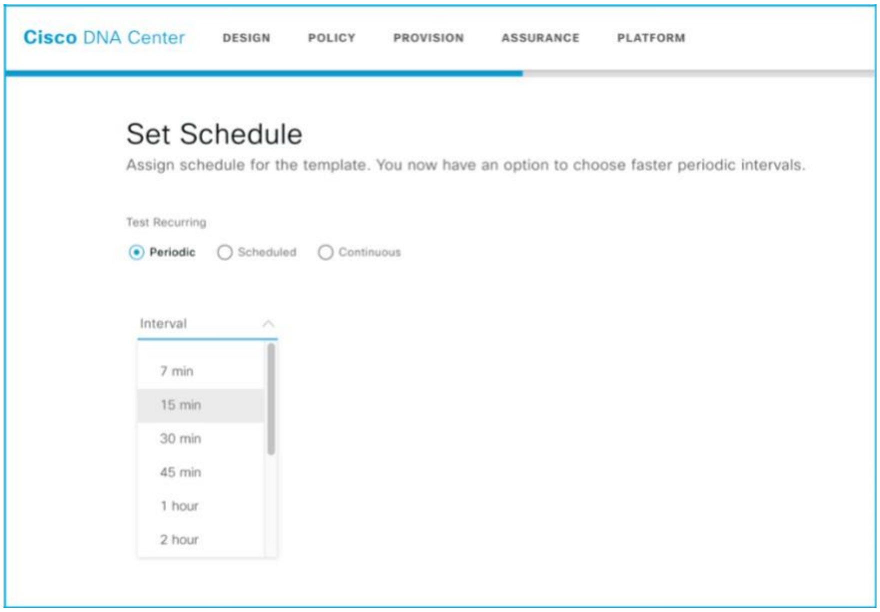
Sensor belongs to test. Applying a new template will overwrite it.

Target AP	Band: RSSI	
□ AP4800.90A4	2.4GHz : -	5GHz : -
□ AP9120.CF6C	2.4GHz : -	5GHz : -
□ AP9120.B848	2.4GHz : -	5GHz : -
□ AP4800.6DEC	2.4GHz : -	5GHz : -

☑ Sensor Candidate	Target AP #
☑ SJC-B4-06 ⚠	4
☑ SJC-B4-05 ⚠	4
☑ SJC-B4-04 ⚠	4
☑ SJC-B4-03 ⚠	4
☑ SJC-B4-02 ⚠	4

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.



Set Schedule

Assign schedule for the template. You now have an option to choose faster periodic intervals.

Test Recurring

● Periodic ○ Scheduled ○ Continuous

Interval

- 7 min
- 15 min
- 30 min
- 45 min
- 1 hour
- 2 hour

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.

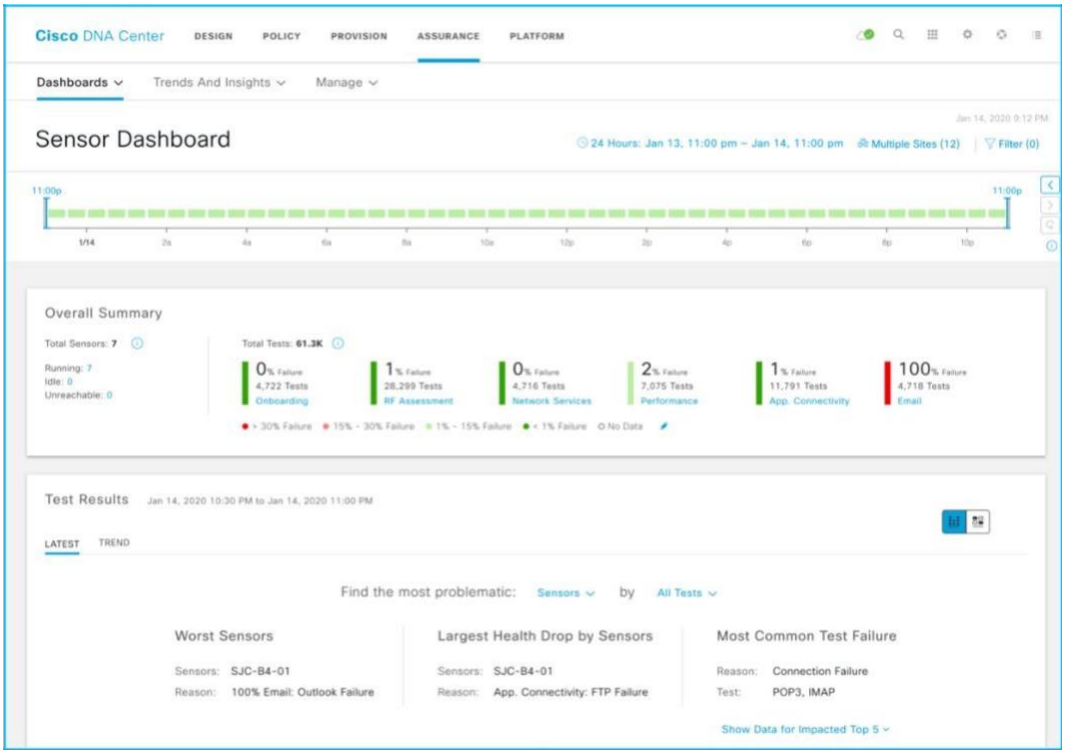
Monitor Sensor Health

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



Sensor Dashboard

Jan 14, 2020 9:12 PM

24 Hours: Jan 13, 11:00 pm – Jan 14, 11:00 pm   Multiple Sites (12)   Filter (0)

Overall Summary

Total Sensors: 7

Running: 7
Idle: 0
Unreachable: 0

Total Tests: 61.3K

0% Failure 4,722 Tests Onboarding

1% Failure 28,299 Tests RF Assessment

0% Failure 4,716 Tests Network Services

2% Failure 7,075 Tests Performance

1% Failure 11,791 Tests App. Connectivity

100% Failure 4,718 Tests Email

● > 30% Failure ● 15% - 30% Failure ● 1% - 15% Failure ● < 1% Failure ○ No Data

Test Results Jan 14, 2020 10:30 PM to Jan 14, 2020 11:00 PM

Find the most problematic: Sensors by All Tests

Worst Sensors
Sensors: SJC-B4-01
Reason: 100% Email: Outlook Failure

Largest Health Drop by Sensors
Sensors: SJC-B4-01
Reason: App. Connectivity: FTP Failure

Most Common Test Failure
Reason: Connection Failure
Test: POP3, IMAP

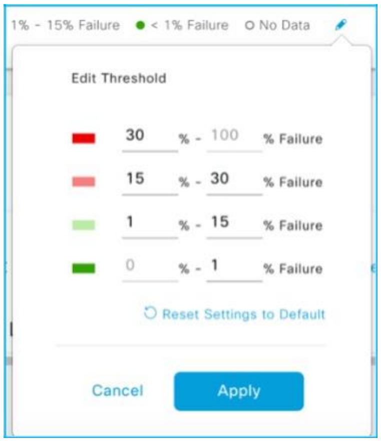
Show Data for Impacted Top 5

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: P**rovides 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.



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

Edit Threshold

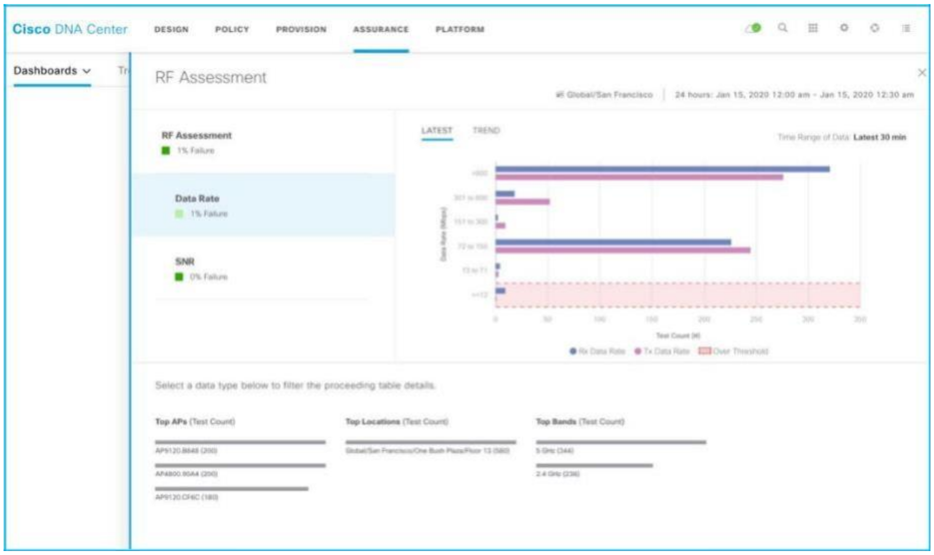
🟥	30 % -	100	% Failure
🟥	15 % -	30	% Failure
🟩	1 % -	15	% Failure
🟩	0 % -	1	% Failure

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



RF Assessment

Global/San Francisco | 24 hours: Jan 15, 2020 12:00 am - Jan 15, 2020 12:30 am

RF Assessment
🟩 1% Failure

Data Rate
🟩 1% Failure

SNR
🟩 0% Failure

Time Range of Data: **Latest 30 min**

Select a data type below to filter the proceeding table details.

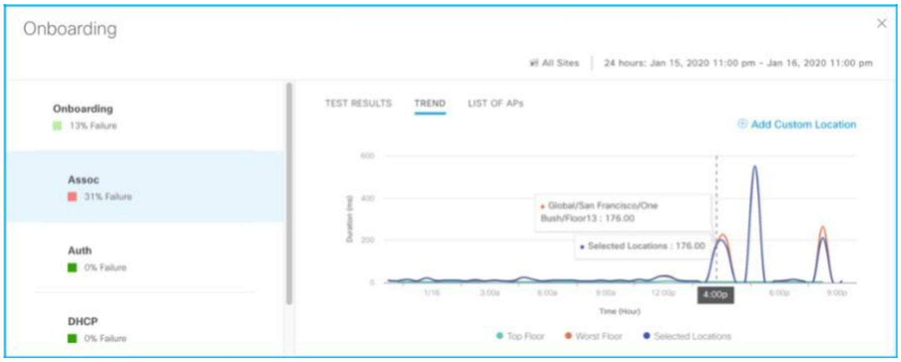
Top APs (Test Count)
AP9120.B848 (200)
AP4800.90A4 (200)
AP9120.CF6C (180)

Top Locations (Test Count)
Global/San Francisco/One Bush Plaza/Floor 13 (580)

Top Bands (Test Count)
5 GHz (344)
2.4 GHz (236)

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.



Onboarding

All Sites | 24 hours: Jan 15, 2020 11:00 pm - Jan 16, 2020 11:00 pm

Onboarding
🟩 13% Failure

Assoc
🟥 31% Failure

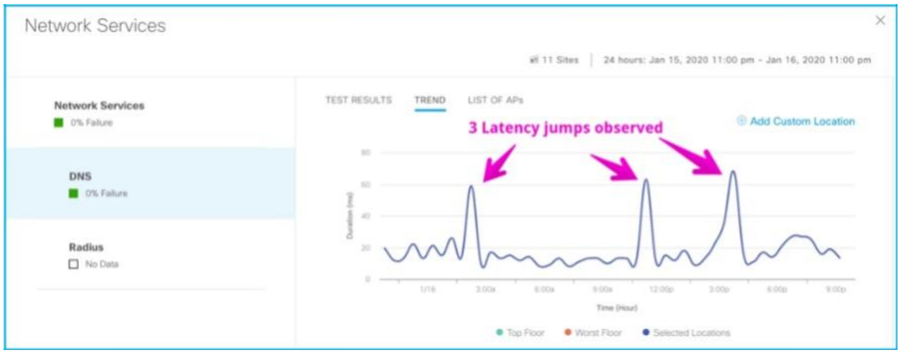
Auth
🟩 0% Failure

DHCP
🟩 0% Failure

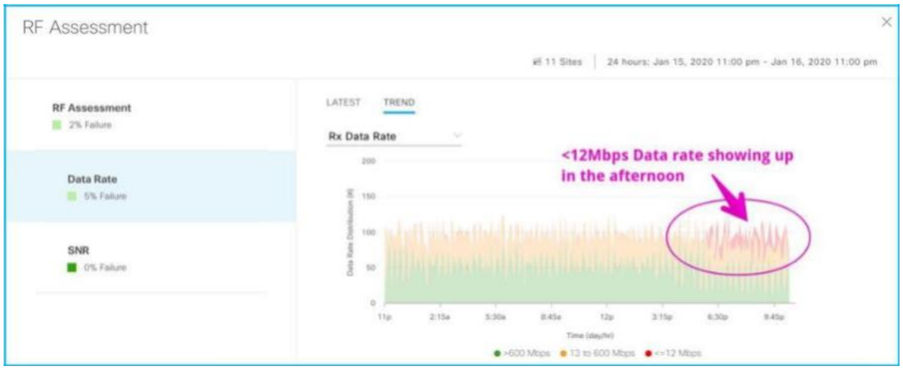
Global/San Francisco/One Bush/Floor13 : 176.00

Selected Locations : 176.00

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.

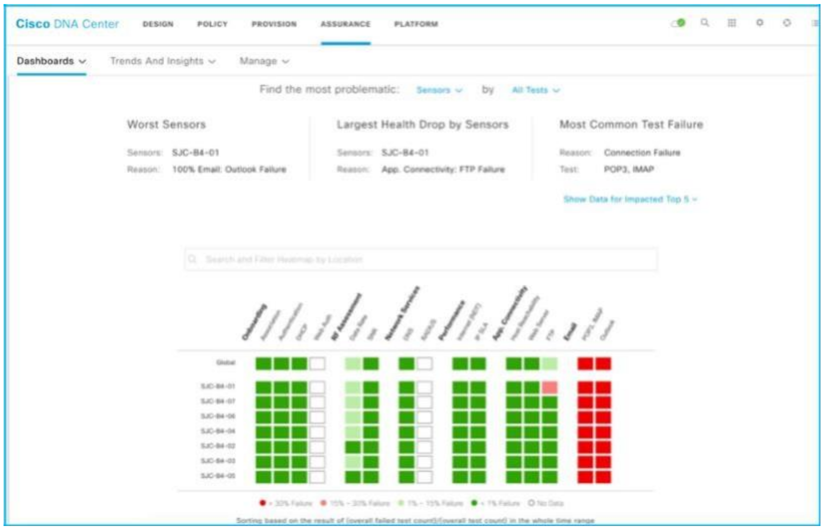


For example, this DNS test result shows 3 spikes on the DNS response during the last 24 hours.



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



Find the most problematic: Sensors by All Tests

Worst Sensors
Sensors: SJC-B4-01
Reason: 100% Email: Outlook Failure

Largest Health Drop by Sensors
Sensors: SJC-B4-01
Reason: App. Connectivity: FTP Failure

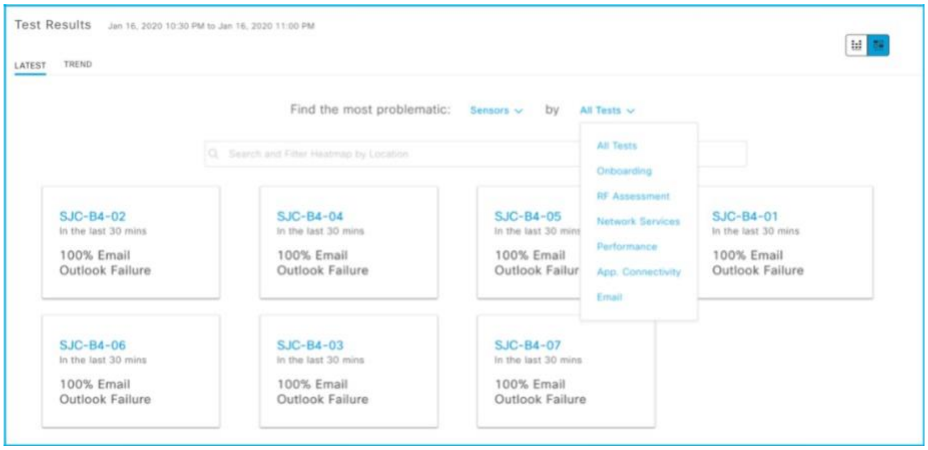
Most Common Test Failure
Reason: Connection Failure
Test: POP3, IMAP

Show Data for Impacted Top 5

Sorting based on the result of (overall failed test count)/(overall test count) in the whole time range

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.



Test Results Jan 16, 2020 10:30 PM to Jan 16, 2020 11:00 PM

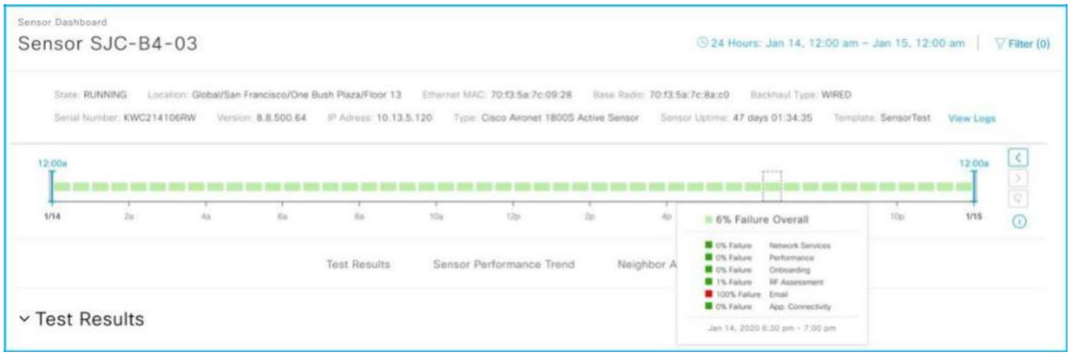
Find the most problematic: Sensors by All Tests

SJC-B4-02 In the last 30 mins 100% Email Outlook Failure	SJC-B4-04 In the last 30 mins 100% Email Outlook Failure	SJC-B4-05 In the last 30 mins 100% Email Outlook Failur	SJC-B4-01 In the last 30 mins 100% Email Outlook Failure
SJC-B4-06 In the last 30 mins 100% Email Outlook Failure	SJC-B4-03 In the last 30 mins 100% Email Outlook Failure	SJC-B4-07 In the last 30 mins 100% Email Outlook Failure	

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.



Sensor Dashboard

Sensor SJC-B4-03

24 Hours: Jan 14, 12:00 am – Jan 15, 12:00 am | Filter (0)

State: RUNNING Location: Global/San Francisco/One Bush Plaza/Floor 13 Ethernet MAC: 70:f3:5a:7c:09:28 Base Radio: 70:f3:5a:7c:8a:c0 Backhaul Type: WIRED

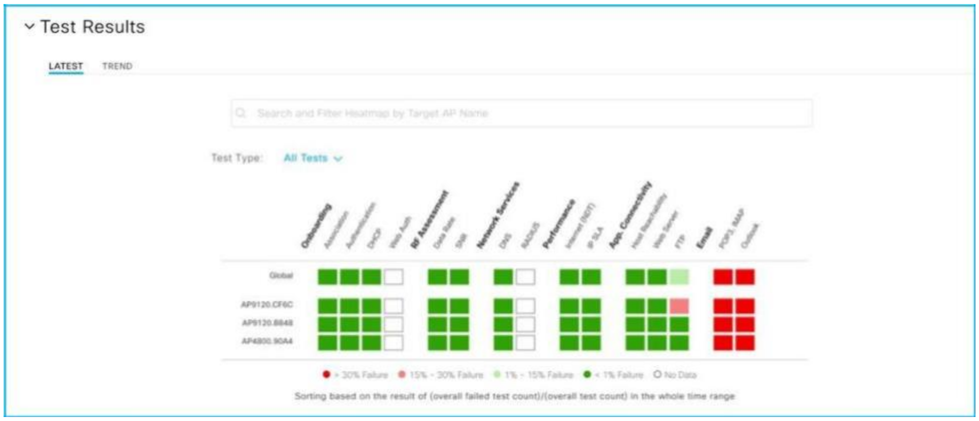
Serial Number: KWC214106RW Version: 8.8.500.64 IP Adress: 10.13.5.120 Type: Cisco Aironet 1800S Active Sensor Sensor Uptime: 47 days 01:34:35 Template: SensorTest View Logs

6% Failure Overall

🟩 0% Failure	Network Services
🟩 0% Failure	Performance
🟩 0% Failure	Onboarding
🟩 1% Failure	RF Assessment
🟥 100% Failure	Email
🟩 0% Failure	App. Connectivity

Jan 14, 2020 6:30 pm - 7:00 pm

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.



Test Results

LATEST TREND

Search and Filter Heatmap by Target AP Name

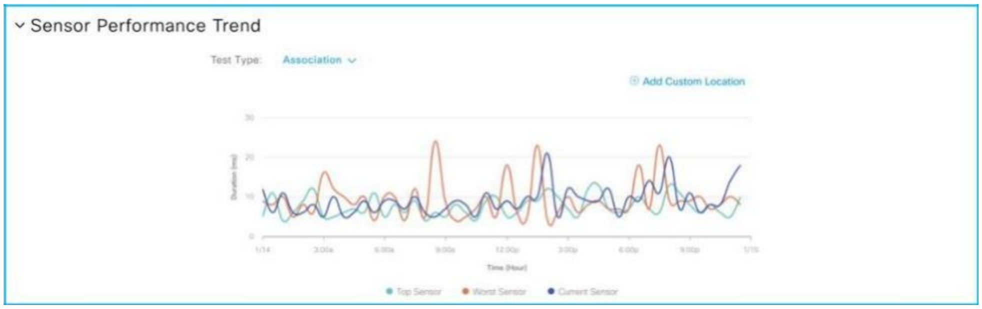
Test Type: All Tests

	Onboarding: Association	Authentication	DHCP	Web Auth	RF Assessment: Data Rate	SNR	Network Services: DNS	RADIUS	Performance: Internet (NDT)	IP SLA	App. Connectivity: Host Reachability	Web Server	FTP	Email: POP3, IMAP	Outlook
Global	🟩	🟩	🟩	□	🟩	🟩	🟩	□	🟩	🟩	🟩	🟩	▧	🟥	🟥
AP9120.CF6C	🟩	🟩	🟩	□	🟩	🟩	🟩	□	🟩	🟩	🟩	🟩	▨	🟥	🟥
AP9120.B848	🟩	🟩	🟩	□	🟩	🟩	🟩	□	🟩	🟩	🟩	🟩	🟩	🟥	🟥
AP4800.90A4	🟩	🟩	🟩	□	🟩	🟩	🟩	□	🟩	🟩	🟩	🟩	🟩	🟥	🟥

🟥 > 30% Failure ▨ 15% - 30% Failure ▧ 1% - 15% Failure 🟩 < 1% Failure □ No Data

Sorting based on the result of (overall failed test count)/(overall test count) in the whole time range

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.

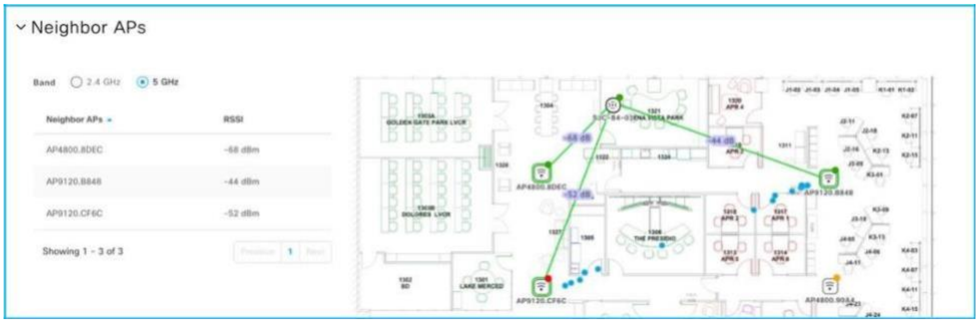


Sensor Performance Trend

Test Type: Association

⊕ Add Custom Location

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.



Neighbor APs

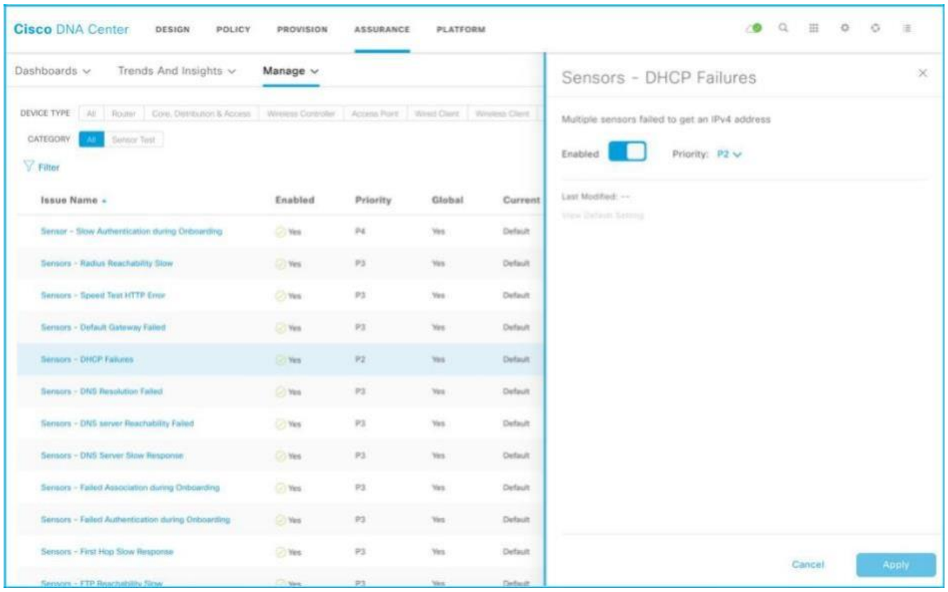
Band ○ 2.4 GHz ● 5 GHz

Neighbor APs	RSSI
AP4800.8DEC	-68 dBm
AP9120.B848	-44 dBm
AP9120.CF6C	-52 dBm

Showing 1 - 3 of 3 Previous 1 Next

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



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

Sensors - DHCP Failures

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.

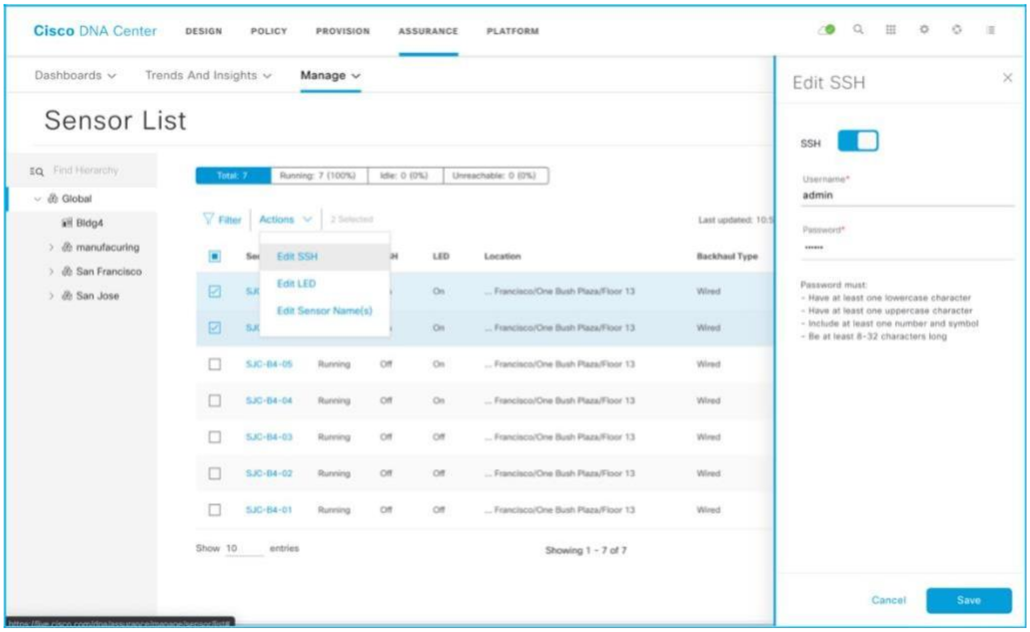
You can customize the priority or turn on or off any sensor issue type. In Cisco DNA Center Release 1.3.3, sensor issues are also exportable from the **Issue Dashboard** page.

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.



Sensor List

Find Hierarchy
- Global
  - Bldg4
  - manufacuring
  - San Francisco
  - San Jose

Total: 7 | Running: 7 (100%) | Idle: 0 (0%) | Unreachable: 0 (0%)

Filter | Actions | 2 Selected | Last updated: 10:5

Actions: Edit SSH, Edit LED, Edit Sensor Name(s)

■	Se		H	LED	Location	Backhaul Type
☑	SJ			On	... Francisco/One Bush Plaza/Floor 13	Wired
☑	SJ			On	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-05	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-04	Running	Off	On	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-03	Running	Off	Off	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-02	Running	Off	Off	... Francisco/One Bush Plaza/Floor 13	Wired
□	SJC-B4-01	Running	Off	Off	... Francisco/One Bush Plaza/Floor 13	Wired

Show 10 entries

Showing 1 - 7 of 7

Edit SSH

SSH: on

Username*: admin

Password*: ••••••

Password must:
- Have at least one lowercase character
- Have at least one uppercase character
- Include at least one number and symbol
- Be at least 8-32 characters long

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.

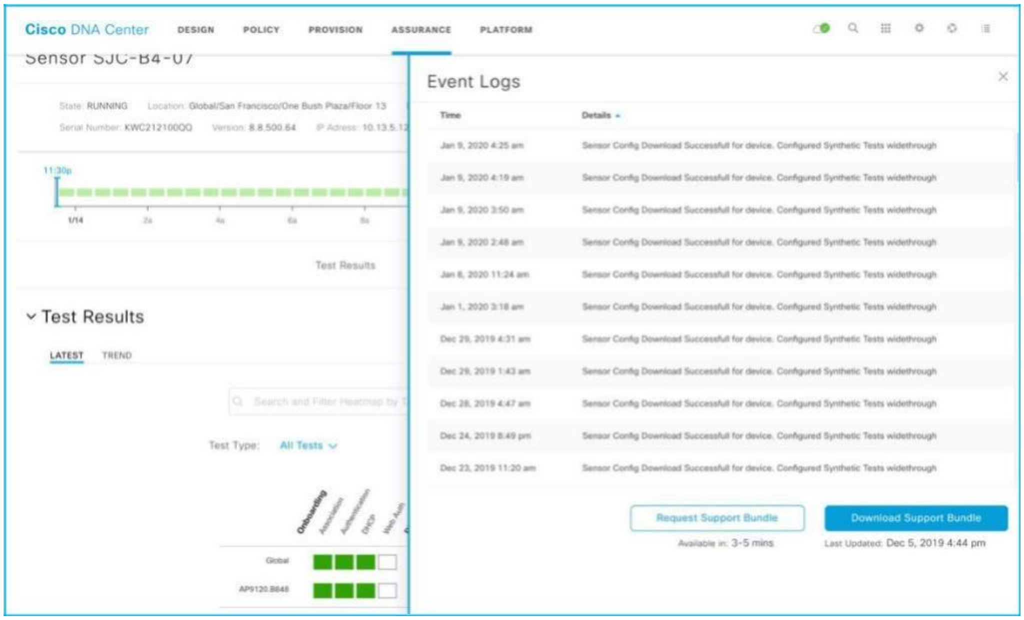
Sensor specific commands have a prefix of `show/config dot11` sensor command line, as shown in the following example:

```
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.



Sensor SJC-B4-07

State: RUNNING Location: Global/San Francisco/One Bush Plaza/Floor 13
Serial Number: KWC212100QQ Version: 8.8.500.64 IP Adress: 10.13.5.12

Test Results

Test Type: All Tests

Event Logs

Time	Details
Jan 9, 2020 4:25 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Jan 9, 2020 4:19 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Jan 9, 2020 3:50 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Jan 9, 2020 2:48 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Jan 8, 2020 11:24 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Jan 1, 2020 3:18 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Dec 29, 2019 4:31 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Dec 29, 2019 1:43 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Dec 28, 2019 4:47 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Dec 24, 2019 8:49 pm	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough
Dec 23, 2019 11:20 am	Sensor Config Download Successfull for device. Configured Synthetic Tests widethrough

Available in: 3-5 mins

Last Updated: Dec 5, 2019 4:44 pm

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.

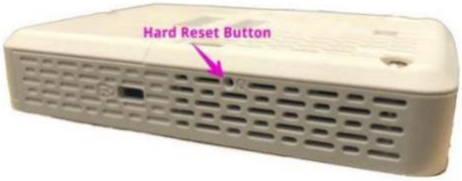
Reset Sensor Configuration

To rest 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,
--More—
```

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)

`#config dot11 sensor pnp ip 192.168.0.100`	Prime DNAC's IP address (192.168.0.100) statically

`# show pnp info`
`PI version: 1.8.0.dev20`
`PD version: 1.5.2.dev2`
	Show the pnp agent version.

`# show pnp status`	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