Manage Sensors and Sensor-Driven Tests

About Sensors and Sensor-Driven Tests

Sensors use sensor-driven tests to determine the health of wireless networks. A wireless network includes AP radios, WLAN configurations, and wireless network services.

Assurance supports a dedicated sensor, which is dedicated hardware for performing sensor functions.

The dedicated Cisco Aironet 1800s Active Sensor gets bootstrapped using PnP. After this sensor obtains Assurance server-reachability details, it directly communicates with the Assurance server.

Supported Sensor and Cisco Wireless Controller Software Releases

The sensor functionality requires the following minimum software versions of Cisco Wireless Controllers and Cisco Aironet 1800s Active Sensor images:

Supported Sensor and Wireless Controllers	Minimum Software Release
Cisco Wireless Controller (35xx, 55xx, 85xx)	8.5.115.0
Cisco Catalyst 9800 Wireless Controller	IOS-XE 16.12.1s or later
Cisco Aironet 1800s Active Sensor	8.8.263.0

Provision Sensors

Provision the Wireless Cisco Aironet 1800s Active Sensor

Step 1 If you are using the Cisco Aironet AP 1800S Sensor without an Ethernet module, you must enable `CiscoProvisioningSSID` on the wireless controller.

> **Note** For the Cisco Aironet 1800s Active Sensor earlier than Software Release 1.3.1.2, make sure that you do not choose the sensor device profile **`CiscoProvisioningSSID`**. Instead, choose your own SSID for backhaul purposes. See Manage Backhaul Settings, on page 15.

For Cisco Wireless Controllers, see Enable Provisioning SSID on the Wireless Controller, on page 2.

For Cisco Catalyst Wireless Controllers, see Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller, on page 3.

Step 2 Create a backhaul configuration for the sensor.

See Manage Backhaul Settings, on page 15.

Step 3 Provision the Cisco Aironet 1800s Active Sensor.

See Provision a Wireless or Sensor Device, on page 4.

Step 4 (Optional) After the sensor device is available in the device inventory, you can choose to upgrade the software image. See the "Provision Software Images" topic in the *Cisco DNA Center User Guide*.

Enable Provisioning SSID on the Wireless Controller

Step 1 Log in to the Cisco Wireless Controller.

The **Network Summary** page appears.

Step 2 Click the **Advanced** tab.

The **Summary** page appears.

Step 3 In the top menu bar, click the **Management** tab.

Step 4 From the left-navigation pane, choose **Cloud Services** > **Sensor**.

The **Backhaul Configuration** page appears.

Step 5 In the **SSID** field, enter **`TFTP`**.

Step 6 From the **Auth-type** drop-down list, choose **Open**.

Step 7 From the **Provisioning** drop-down list, choose **Enable**.

Step 8 Make sure that the **DHCP Interface** drop-down list is set to **management**.

Step 9 Click **Apply**.

After provisioning is enabled, a hidden WLAN called `CiscoSensorProvisioning` is created, and the sensor joins using an EAP-TLS client certificate. This enables the sensor to find the Cisco DNA Center IP address, which is done using DHCP Option 43 or through DNS.

Enable Cisco Provisioning SSID on the Cisco Catalyst Wireless Controller

Step 1 Log in to the Cisco Catalyst Wireless Controller GUI.

Step 2 From the left-navigation pane, choose **Configuration** > **Cloud Services**.

The **Cloud Services** page appears.

Step 3 In the **Network Assurance** tab, do the following:

a) From the **Network Assurance Configuration** area, set the **Service Status** toggle to **Enabled**.

b) From the **Provisioning** area, set the **Provisioning** toggle to **Enabled**.

Step 4 (Optional) In the **VLAN Interface** field, enter the name of the VLAN interface.

Step 5 Click **Apply**.

After Provisioning is enabled, a hidden WLAN called **CiscoSensorProvisioning** is created.

The following error message appears in the bottom-right corner of the window.

Error in Configuring
CLI Line 2 Please associate the wlan and policy profile CiscoSensorProvisioning to the desired AP.

Note This message is not an error. The message provides information about the action that must be performed.

Step 6 Verify that the **CiscoSensorProvisioning** policy profile is created.

a) From the left-navigation pane, choose **Configuration** > **Policy**.

The **Policy Profile** page appears.

b) Verify that the **CiscoSensorProvisioning** policy appears under the **Policy Tag Name** column.

Step 7 Associate the WLAN and policy profile **CiscoSensorProvisioning** to the appropriate AP. Do the following:

a) From the left-navigation pane, choose **Configuration** > **Tags**.
The **Manage Tags** page appears.

b) In the **Policy** tab, click **Add**.

c) In the **Name** field, enter a unique name for the Policy Tag.

d) Click **Add**.

e) From the **WLAN Profile** drop-down list, choose **CiscoSensorProvisioning**.

f) From the **Policy Profile** drop-down list, choose **CiscoSensorProvisioning**.

g) Click ✔.

h) Click **Save & Apply to Device** to save the Policy Tag.

Note Changing the Policy Tag on an AP may cause clients associated with the AP to disconnect and reconnect.

Provision a Wireless or Sensor Device

This procedure explains how to claim a device from the Plug and Play Devices list. Alternatively, you can claim a device from the device details window by clicking **Claim**.

Before you begin

- Ensure that Cisco network devices to be provisioned have a supported software release and are in a factory default state. If you are using a network device that was previously configured or is in an unknown state, see the device clean-up and reset details in the Network Plug and Play Troubleshooting Guide for Cisco DNA Center.

- Define the site within the network hierarchy. See Design Network Hierarchy.

- Define the CLI and SNMP credentials for the devices.

> **Note** You can claim wireless devices using CLI, SNMPv2c, or SNMPv3 credentials. If you use SNMPv2c, provide both Read Only and Read Write credentials.

- Optionally, ensure that the software images for any Cisco Catalyst 9800-CL devices to be provisioned are uploaded and marked as golden in the Image Repository, if you want to deploy images.

> **Note** The image deployment process used by Plug and Play during Day-0 provisioning is not the same as that used when updating a device image later. During Plug and Play provisioning, there are no device prechecks, auto flash cleanup, or postchecks done, as it is expected that devices are in the factory default state.

- For provisioning a sensor device, ensure that the sensor is reachable through the Cisco DNA Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Cisco DNA Center; however, to claim the device, it must be reachable from the interface enp9s0 IP address. In the DHCP server, configure the NTP server (DHCP option 42) and the vendor-specific DHCP option 43 with ACSII value "5A1D;B2;K4;I172.16.x.x;J80;", where 172.16.x.x is the virtual IP address of Cisco DNA Center associated with the enp9s0 interface.

Step 1 From the top-left corner, click the menu icon and choose **Provision** > **Plug and Play**.

Step 2 View the devices in the table.

You can use the search bar to find specific devices.

Step 3 Check the check box next to the device or devices that you want to claim.

Step 4 From the menu bar above the device table, choose **Actions** > **Claim**.

Step 5 (Optional) In the **Assign Site** window, do the following:

a) Change the device hostname, if needed.

b) Assign a site by doing any of the following:

- To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, choose a site.

- To assign the same site as the first device to all other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **Apply Site to All**.

- To assign a site from any device to some other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **Assign this Site to Other Devices**, choose the devices, and click **Assign**.

- To clear the site assigned to the devices, click **Clear Site**.

If the wireless network profile associated with the assigned site has an onboarding template, Cisco DNA Center uses this template for PnP onboarding.

Note   In the **System** > **Settings** > **Device Settings** > **PnP AP Location** window:

- If the **Configure AP Location** check box is checked, Cisco DNA Center assigns this site as the AP location during PnP onboarding.

- If the **Configure AP Location** check box is unchecked, Cisco DNA Center does not configure this site as the AP location during PnP onboarding. You can configure the AP location using the **Configure Access Points** workflow.

For more information, see "Configure AP Location for PnP Onboarding" in the *Cisco DNA Center Administrator Guide*.

c)   Click **Next**.

Step 6   In the **Assign Configuration** window, do the following:

a)   In the **Configuration** column, click **Assign** for the device that you want to configure.

b)   If the device configuration doesn't need any changes, click **Cancel** and proceed to next step. Otherwise, change or configure any of the following settings:

- **Device Name**: Change the device hostname, if needed.

- **Image**: From this drop-down list, choose a golden software image to apply to the device. If there is only one golden image for this device type in the image repository, it is chosen by default.

- **Template**: From this drop-down list, choose an onboarding configuration template to apply to the device. If there is only one onboarding configuration template defined for this device type, it is chosen by default.

  Note   If you have not assigned the device to a site, you must choose a template for the device to proceed further.

- **Catalyst Wireless LAN Controller Settings**: For a wireless controller, enter values in the following fields: **Wireless management IP**, **Subnet mask**, **Gateway**, **IP interface name**, and optionally, **VLAN ID**.

  If you are on a Cisco DNA Center controller that has an IPv6 address, you must enter IPv6 values for the first three fields. If you are on a controller that has an IPv4 address, you must enter IPv4 values for these fields.

- For an AP device, in the **Radio Frequency Profile** drop-down list, choose a radio frequency profile to apply to the device. This may be set if you designated one profile as a default.

- For a Mobility Express device, enter values in the following fields: **Wireless management IP**, **Subnet mask**, and **Gateway**.

- For a wireless sensor device, in the **Sensor Settings** drop-down list, choose the sensor device profile (backhaul) to apply to the device.

Note	For Cisco Aironet 1800s Active Sensor earlier than Release 1.3.1.2, make sure that you do not choose the sensor device profile `CiscoProvisioningSSID`. Instead, choose your own SSID for backhaul purposes.

- If you made any changes, click **Save**; otherwise, click **Cancel** to return to the list and configure other devices.

c) From the **Clear Configuration** drop-down list, choose any the following options:

- **Clear Device Certificates**: Choose this option and check the check box adjacent to each of the devices that you want to clear the certificate from, and click **Clear**.

- **Clear Images**: Choose this option and check the check box adjacent to each of the devices that you want to clear the image from, and click **Clear**.

- **Clear Templates**: Choose this option and check the check box adjacent to each of the devices that you want to clear the template from, and click **Clear**.

- **Clear License Levels**: Choose this option and check the check box adjacent to each of the devices that you want to clear the license level from, and click **Clear**.

d) To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon ••• and choose **Apply Image to Other Devices** or **Apply Template to Other Devices**.

For wireless controller devices, you can apply the device license level to other devices by clicking **Apply License Level to Other Devices**.

e) If you selected multiple devices to provision, click **Assign** for the next device in the list and repeat the configuration steps, until you have done this for all devices.

f) After you have configured all the devices, click **Next**.

Step 7 In the **Provision Templates** window, select the template from **Devices** area and enter your domain name in **domain** field and click **Next**.

Step 8 In the **Summary** window, view details about the devices and their configuration preview.

Step 9 Check the **Device Configuration** column for each device to see if the configuration preview was successful.

If the preview shows an error, you can click the **Actions** link in the error message above the table to see what actions you need to take. You can click an action to open a new tab with the window where a change is needed. You must resolve any issues before claiming the device, to avoid provisioning errors. You may need to go back to the **Assign Configuration** step and change the configuration, revisit the **Design** area to update network design settings, or resolve any network connectivity issues. After you have resolved the problem, you can go back to this tab, click **Retrying getting Day-0 configuration preview for failed device(s)**, and click **OK**. Ensure that the wireless controller that is managing a device has been added to the inventory and assigned to the site where the wireless device is assigned.

Step 10 In the **Device Configuration** column, click **Preview Configuration** to review the configuration.

Step 11 Click **Claim**.

Step 12 In the confirmation dialog box, click **Yes** to claim the devices and start the provisioning process.

Note	If there is a conflicting operation for the selected site, to proceed with the current configuration, you must either wait for the existing, scheduled, or pending-review operations to complete or discard the operations.

What to do next

If you have configured network settings, provision these settings on the devices. For more information, see the "Complete the Provisioning Process" in the *Cisco DNA Center User Guide*

Monitor and Troubleshoot Network Health with Sensors

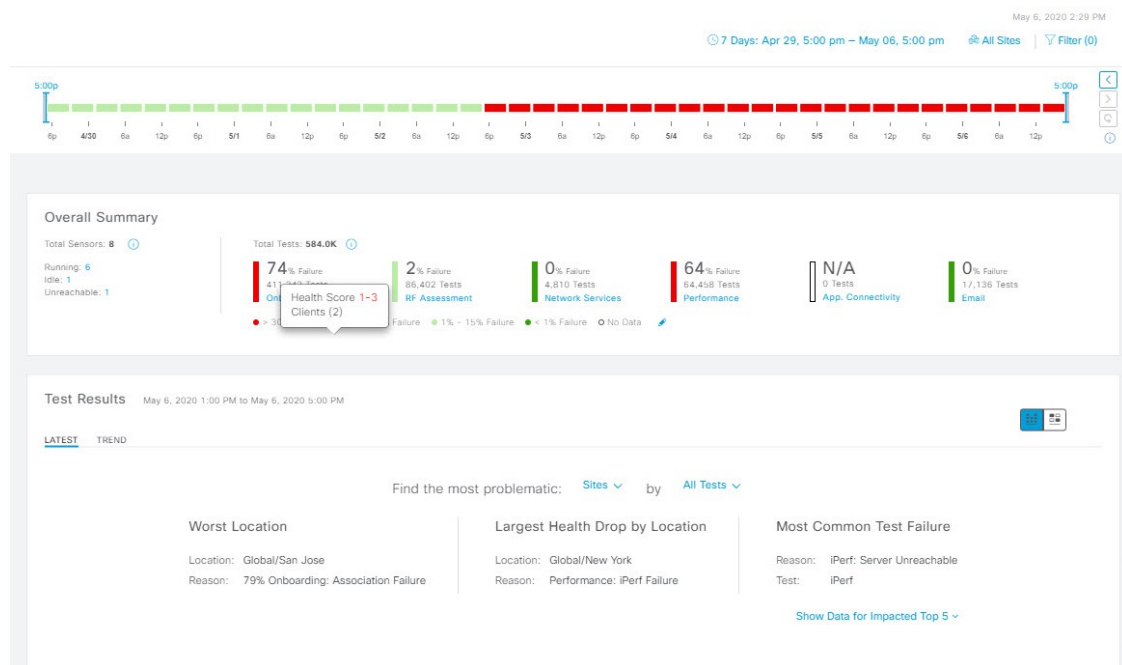## Monitor and Troubleshoot Network Health with All Wireless Sensors

Use this procedure to get a global view of the network health from the data received from all wireless sensors.

Before you begin

Make sure you have added and scheduled sensor-driven tests. See Create and Run Sensor-Driven Tests Using Templates, on page 22.

Step 1   From the top-left corner, click the menu icon and choose **Assurance** > **Dashboards** > **Wireless Sensors**.

Figure 1: Wireless Sensors Dashboard

Step 2   Use the **Wireless Sensors** dashboard top-menu bar for the following functionality:

Timeline Area	
Item	**Description**
🕐 **Time Range** setting	Enables you to display data within a specified time range on the dashboard. Do the following: **a.** From the drop-down menu, choose the length of the range: **3 Hours**, **24 Hours**, or **7 Days**. **b.** Specify the **Start Date** and time; and the **End Date** and time. **c.** Click **Apply**.
🏛 **Hierarchy Location** setting	Enables you to choose the data displayed on the dashboard from the selected locations in your network. Check the check boxes for the sites, buildings, or floors in your network to display its sensor data on the dashboard. **Note** You can't exclude all locations from displaying data on the dashboard. Unchecking all locations results in data from all locations to be displayed on the dashboard.
Filter icon	Enables you to choose the data displayed on the dashboard based on SSIDs and radio frequency bands. To add filters: **a.** Click **Filter**. **b.** From the drop-down menu, click the **SSID** tab and check the check boxes for the desired SSIDs. **c.** From the drop-down menu, click the **Band** tab and select the radio button for **2.4 GHz** or **5 GHz**. **d.** Click **Apply**. To remove all selected filters: **a.** Click the **Filter** icon. **b.** Click **Clear Filters**.

Step 3 Use the **Timeline** to view the percentage of overall test failures for a specific time within a time range.

The time range is determined by what is configured in the 🕐 setting above the timeline.

The blocks in the timeline represents a specific time window within the time range. The period of time for each block is determined by time range set for the timeline:

- For a **3 Hours** time range, each block represents 15 minutes.

- For a **24 Hours** time range, each block represents 30 minutes.

- For a **7 Days** time range, each block represents 4 hours.

The blocks are color-coded to indicate the severity of percentage of test failures.

Hover your cursor over a block to view a breakdown of percentage of test result failures for each test category.

Step 4 Use the **Overall Summary** dashlet for the following functionality:

Overall Summary Dashlet	
Item	**Description**
Total Sensors area	Provides an overall view of all the sensors in your network and their status. The following are the status types of the sensor: • **Idle**: The sensor is onboarded and does not have any scheduled tests. • **Running**: The sensor is onboarded and is included in a test suite or test template. • **Unreachable**: No heartbeat received from the sensor. Click the hyperlinked number next to the status type to open a slide-in pane that displays the sensors with that status. In the slide-in pane, you can click the sensor name under the **Name** column to get a 360° view of that sensor. See Monitor and Troubleshoot Network Health with a Wireless Sensor, on page 11.

Total Tests	Displays the total number of tests performed by all sensors and a breakdown of the test results based on the following test categories:
	
	Onboarding
	RF Assessment
	Network Services
	Performance
	App. Connectivity
	Email
	
	You can click a test category to open a slide-in pane with additional details about its test results.
	
	In the slide-in pane, click the test type tabs on the left to populate the slide-in pane with data from the test type. The slide-in pane displays the following:
	
	• A chart that displays the test results, future trends, and list of APs used in the tests.
	
	    Note For the **RF Assessment** test category, the chart displays the KPIs data rate and SNR, instead of test results.
	
	• Data type categories: **Top Failure Reasons** (if applicable), **Top APs**, **Top Locations**, **Top Bands**, and **Top SSIDs** (if applicable).
	
	• A table with detailed data of the sensors that ran the tests.
	
	    You can click the data segments from the data type categories to filter the data that appears in the table.

Overall Summary Dashlet	
Item	**Description**
✏️ **Edit Threshold**	Enables you to customize the thresholds of the color-coded ranges that indicate the severity of percentage of test result failures. 🔴 > 30% Failure 🔴 15% – 30% Failure 🟢 1% – 15% Failure 🟢 < 1% Failure To customize the thresholds: a. Click the edit (✏️) icon. b. In the **Edit Threshold** menu, enter the percentage values in the fields for each color-coded range. c. Click **Apply**.

Step 5 Use the **Test Results** dashlet to view the locations in your network with the most sensor test result failures:

Test Results Dashlet	
Item	**Description**
Latest tab and **Trend** tab	These tabs determine the scope of the data that is displayed in the dashlet: • **Latest**: Displays the data from the selected time window in the timeline on the top of the window. • **Trend**: Displays data from the last 24 hours.
🔲🔲 **Heatmap View** and **Card View** toggle	This toggle button allows you to change the view of the dashlet to the **Heatmap View** and the **Card View**. The **Heatmap View** is displayed by default.

Test Results Dashlet	
Item	**Description**
⊞ **Heatmap View**	Displays the top 5 rankings of the following statistical categories at the top of the dashlet: • **Worst Location, Buildings, Floors,** or **Sensors**: Sites, buildings, floors, or sensors with the highest test result failure percentage. • **Largest Health Drop by Location, Buildings, Floors,** or **Sensors**: Sites, buildings, floors, or sensors with the largest sudden drop. • **Most Common Test Failure**: Test types that had the highest test result failures. Only the top spot for each statistical category is displayed. Click **Show Data for Impact Top 5** to see the complete rankings. Below the rankings is a heatmap representation of the sensor test result failures. In the heatmap, the blocks are color-coded to indicate the severity of percentage of test result failures. • Use the drop-down lists in the **Find the most problematic** area to sort the data that is displayed in the rankings and heatmap. In the first drop-down list you can sort the data by locations or sensors. In the second drop-list you can sort the data by test types. • Use the search field to filter the heatmap for specific locations or sensors. • Hover your cursor over a block to view the exact percentage value for test result failures. • Click a color-coded block to open a slide-in pane with further details about the test results at that intersect.
⊞ **Card View**	Displays the data in a card format for high-level monitoring and comparison. Use the drop-down lists in the **Find the most problematic** area to sort the data.

Monitor and Troubleshoot Network Health with a Wireless Sensor

Use this procedure to get a 360° view of a specific wireless sensor. You can view a sensor's test results, performance trends, and neighboring APs. You can also view and download a sensor's event logs.

Step 1   From the top-left corner, click the menu icon and choose **Assurance** > **Dashboards** > **Wireless Sensors**.

The **Sensor Dashboard** appears.

Step 2   From the **Sensors Dashboard**, do one of the following:

• In the **Overall Summary** dashlet, click the hyperlinked number from the **Running**, **Idle**, or **Unreachable** areas.

Then in the **Sensor Status** slide-in pane, click the hyperlinked name of the sensor.

• In the **Overall Summary** dashlet, click a hyperlinked test category.

In the slide-in pane, click the hyperlinked name of the sensor from the table.

• In the **Test Results** dashlet, click a color-coded box from the heatmap.

In the slide-in pane, click the hyperlinked name of the sensor from the table.

A 360° view of the sensor appears.

Step 3 Click the 🕐 **Time Range** setting at the top-right corner to specify the time range of data that is displayed on the window:

a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, or **7 days**.
b) Specify the Start date and time; and the End date and time.
c) Click **Apply**.

Step 4 Use the header above the timeline to view the basic information of the sensor such as the sensor's serial number, current state, uptime, backhaul type, IP address, and so on. You can also view and download the sensor's event logs.

To view and download the event logs:

a) Click **View Logs** at the end of the header.
   The **Event Logs** slide-in pane appears which displays the event logs.
b) In the **Event Logs** slide-in pane, click **Request Support Bundle** to generate the support bundle file which contains the event logs.

> **Attention**   It takes about three to five minutes for a support bundle request to be ready for download.

c) Click **Download Support Bundle** to open the download prompt for the support bundle.

Step 5 Use the timeline to view the percentage of overall test failures for a specific time within a specified time range. The timeline has the following functionality:

• Set the time range with the 🕐 **Time Range** setting above the time line.

• View the percentage of overall test failures for a specific time window indicated by the blocks in the timeline. You can hover your cursor over a block to view a breakdown of percentage of test result failures for each test category.

Step 6 Use the collapsible categories to view information about test results, performance trends, and neighboring APs:

Test Results Category

Displays a heatmap representation of the sensor test result failures for each tested AP. In the heatmap, the blocks are color-coded to indicate the severity of percentage of test result failures.
 	
• Use the **Test Type** drop-down list to sort the data by test type.
 	
• Use the search field to filter the heatmap for specific APs.
 	
• Hover your cursor over a block to view the exact percentage value for test result failures.
 	
• Click the **Latest** and **Trend** tabs to change the scope of data displayed in the category:
 	
    • **Latest**: Displays the data from the selected time window in the timeline on the top of the window.
 	
    • **Trend**: Displays data from the last 24 hours.

Sensor Performance Trend Category

Displays a line graph or chart of the sensor performance data based on test types. For time-based test types, a comparative view is used to display the performance of the current sensor, top performing sensor, and worst performing sensor.
 	
  • Use the **Test Type** drop-down list to display data for a specific test type.
 	
  • For time-based test types, click + **Add Custom Location** to add the sensor performance data for a specific location using the menu. You can select the sensor performance for sites, buildings, or floors.

Neighboring APs Category
Displays the sensor's neighboring APs along with its RSSI in a list view and a map view. To filter the APs based on frequency bands, use the radio buttons in the **Band** area. **Note**   The sensor scans for neighboring APs every 30 minutes.

Manage Sensors and Backhaul Settings

Manage Sensors in Your Network

Use this procedure to view the onboarded sensors in your network. You can enable SSH, enable the status LED, and change the name for these sensors.

Before you begin

Make sure the sensors are assigned to a site.

Step 1   From the top-left corner, click the menu icon and choose **Assurance** > **Settings** > **Sensors**.

The **Sensor List** window appears.

Figure 2: Sensor List Window

Step 2 Use the left pane to specify the network hierarchy you want to view.

Step 3 Click the categories above the table to view the sensors that fit its criteria. The categories are:

- **Total**: All the sensors in the selected network hierarchy.

- **Running**: Displays the sensors that are currently running tests.

- **Idle**: Displays the sensors that have no assigned tests.

- **Unreachable**: Displays the sensors that are onboarded but are not responding to Cisco DNA Center.

Step 4 You can customize the data that is displayed in the table:

a) Click :.

b) From the menu, check the check boxes of the data you want displayed in the table.

c) Click **Apply**.

Step 5 To configure the SSH settings for a sensor, do the following:

a) Check the check box of the sensor.

b) Hover your cursor over the **Actions** drop-down list and choose **Edit SSH**.

The **Edit SSH** slide-in pane appears.

c) In the **Edit SSH** slide-in pane, click the **SSH** toggle to enable SSH.

d) In the **Username** and **Password** fields, enter the desired SSH credentials.

e) Click **Save**.

Step 6 To change the status LED of a sensor, do the following:

a) Check the check box of the sensor.

b) Hover your cursor over the **Actions** drop-down list and choose **Edit LED**.

The **Edit LED** slide-in pane appears.

c) In the **Edit LED** slide-in pane, click the **LED** toggle to enable or disable the status LED.

Step 7   Click **Save**.

Step 8   To change the name of a sensor, do the following:

    a) Check the check box of the sensor.

    b) From the **Actions** drop-down list, choose **Edit Sensor Name(s)**.

       The **Edit Sensor Name(s)** slide-in pane appears.

    c) In the **Edit Sensor Name(s)** slide-in pane, enter the name in the **Name** field.

    d) Click **Save**.

Step 9   To enroll the sensors using SCEP Profiles, do the following:

    a) Check the check box of the sensor.

    b) From the **Actions** drop-down list, choose **Enroll using SCEP**.

       The **Enroll using SCEP** slide-in pane appears.

    c) Choose the SCEP profile from the **Select SCEP Profile** drop-down list.

       See Manage SCEP Profiles for more information.

    d) Select the **Username** and **Password** and provide the required details. If you choose the **Custom** username option, then select **No Password**.

    e) Click **Save**.

    f) To check status, see the **SCEP Profile** column in the **Sensor List** window. A green check mark (✔) indicates success and a red **X** icon indicates failure. Hover your cursor over the ✔ or **X** icon to get more information.

Manage Backhaul Settings

Use this procedure to view, create, and manage backhaul configurations for wireless sensors. A wireless sensor requires a backhaul SSID to communicate with Cisco DNA Center.

For information about a persistent wireless backhaul connection, see Persistent Wireless Backhaul Connections on Sensor Devices, on page 17.

Step 1   From the top-left corner, click the menu icon and choose **Assurance** > **Settings** > **Sensors**.

The **Sensor List** window appears.

Step 2   Hover your cursor over the **Settings** tab and choose **Backhaul Settings**.

Step 3   You can add and manage backhaul SSIDs by doing the following:

    a) Click + **Add Backhaul**.

       The **Create Sensor Backhaul SSID Assignment** window appears with two areas: **Wired Backhaul** and **Wireless Backhaul**.

    b) In the **Settings Name** field, enter a name for the backhaul SSID.

    c) In the **Wired Backhaul** area, configure the following:

        • **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:

           • **802.1x EAP**: Standard used for passing Extensible Authentication Protocol (EAP) over wired LAN.

• **Open**: No security or authentication is used.

• **EAP Method**: If you choose **802.1x EAP**, you must choose one of the following EAP methods for user authentication from the drop-down list:

   • **EAP-FAST**: Enter the username and password in the fields provided.

   • **PEAP-MSCHAPv2**: Enter the username and password in the fields provided.

   • **EAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

   If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click + **Add New Certificate Bundle**, and enter the username and certificate bundle password.

   • **PEAP-TLS**: Choose **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.

   If you choose **Enroll Using Certificate Bundle**, click the drop-down arrow under **Certificate Bundle**, click + **Add New Certificate Bundle**, and enter the username and certificate bundle password.

d) In the **Wireless Network Name (SSID)** area, select the wireless network (SSID) and configure the following.

   • **Level of Security**: Displays the encryption and authentication type used by the selected SSID. The available security options are:

      • **WPA2 Enterprise**: Provides a higher level of security using Extensible Authentication Protocol (EAP) (802.1x) to authenticate and authorize network users with a remote RADIUS server.

      • **WPA2-Personal**: Provides a good security using a passphrase or a preshared key (PSK). This allows anyone with the passkey to access the wireless network.

      If you select **WPA2 Personal**, enter the passphrase in the **Passphrase** text box.

      • **PSK Format**: The available preshared key formats are:

         • **ASCII**: Supports ASCII PSK passphrase.

         • **HEX**: Supports 64-character HEX key PSK password.

      • **Open**: No security or authentication is used.

e) Click **Save**.

Step 4 You can edit the existing backhaul configurations by doing the following:

a) Check the check box of the backhaul configuration.

b) Hover your cursor over the **Actions** drop-down list and choose **Edit**.

Step 5 You can delete a backhaul configuration by doing the following:

a) Check the check box of the backhaul configuration.

b) Hover your cursor over the **Actions** drop-down list and choose **Delete**.

Persistent Wireless Backhaul Connections on Sensor Devices

Cisco DNA Center supports a persistent wireless backhaul connection on sensor devices, which means that the wireless connection is "always on" regardless of wireless testing activities.

- With a dedicated backhaul connection, the wireless sensor uses the following two MAC addresses for backhaul and wireless purposes:

    - Base Radio + 0x10 (Backhaul SSID)

    - Base Radio + 0x11 (Test SSID)

    The wired sensor uses the Base Radio + 0x10 (Test SSID) MAC address for testing purposes.

- The sensor uses *dual* concurrent radio operations, one for the backhaul connection and the other for wireless tests.

- Backhaul connection interruptions occur during scanning and switching interfaces to test different bands.

- The frequency of backhaul connection disruptions is dependent on the test configuration.

- The backhaul connection is not persistent if both backhaul and test SSIDs are in one band.

Manage SCEP Profiles

Use this procedure to view, create, and manage Simple Certificate Enrollment Protocol (SCEP) profiles, which are used to enroll wireless sensors.

Step 1 From the top-left corner, click the menu icon and choose **Assurance** > **Settings** > **Sensors**.

Step 2 Click **Setting** > **SCEP Profiles**.

Step 3 To add and manage a SCEP Profile, do the following:

a) Click **Add SCEP Profiles**.

   The **Create SCEP Profile** window appears.

b) In the **Create SCEP Profile** window, provide the following details:

   - **SCEP Profile Name**: Enter a name for the SCEP profile.

   - **URL Base**: Enter a valid server.

      Note   For **ISE**, enter the following:

                http://*ISE_IP_or_FQDN_Name***:9090/auth/caservice/pkiclient.exe**

                For **Microsoft CA**, enter the following:

                http://*Microsoft_SCEP_IP_or_FQDN_Name***/CertSrv/mscep/mscep.dll**

   - **Common Name**: Enter a valid name.

   - **State**

   - **Country Code**

- **Locality**

- **Organization**

- **Organization Unit**

- **Email**

- **Server certificate fingerprint**

    c) Click **Save**.

Step 4   To edit an existing SCEP Profile, do the following:

    a) Check the check box next to the SCEP Profile.

    b) From the **Actions** drop-down list, choose **Edit**.

Step 5   To delete a SCEP Profile, do the following:

    a) Check the check box next to the SCEP Profile.

    b) From the **Actions** drop-down list, choose **Delete**.

Sensor-Driven Tests

Methods to Create Sensor-Driven Tests in Assurance

In Assurance, there are two methods for creating a sensor-driven test. Choose one of the following methods:

Method	Description
Legacy	You can create sensor-driven tests using the legacy method (also called **Test Suites**).
	See Create and Run Sensor-Driven Tests Using the Legacy Method, on page 18.
Templates	You can create sensor-driven tests using templates.
	With this method, you can create a template of a sensor-driven test, which can be reused for quick deployment to multiple locations in the network.
	See Create and Run Sensor-Driven Tests Using Templates, on page 22.

Create and Run Sensor-Driven Tests Using the Legacy Method

Use this procedure to create and run sensor-driven tests with the legacy method (also called **Test Suites**).

⚠

Warning   The legacy test method will be deprecated in the near future.

Before you begin

If you are using the Cisco Aironet 1800s Active Sensor to run sensor-driven tests, make sure that the sensor is provisioned using PnP, so that it displays under **Inventory**. See Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 2.

Step 1   From the top-left corner, click the menu icon and choose **Assurance** > **Settings** > **Sensors**.

Step 2   Click the **Legacy Tests** tab.

The **Legacy Tests** window appears.

Step 3   To add a new sensor test, click + **Add Test** in the top-right corner.

The **Add Test** window appears.

Step 4   To schedule tests, configure the following settings:

Setting	Description
Test Name field	Enter the name for the test suite. **Note** Use only letters, numbers, underscores, hyphens, and periods.
Location drop-down list	Do the following: a. Choose the sensor location from the drop-down list. b. Check the check boxes of the radios from the SSID you want to add to the test. c. If applicable, configure the **Credentials** settings: **Applicable for WebAuth Enabled SSIDs** For Layer 3 security, if **WebAuth** is enabled on the SSID, provide the following: • For **WebAuth** with user authentication, provide the necessary credentials. • For **WebAuth** with **Passthrough**, you can choose to provide an email address. **Note** • Only **Internal Authentication** is supported for sensor testing. • WebAuth is supported on Cisco Wireless Controllers and Cisco Aironet 1800s Active Sensors with Software Release 8.7. **Applicable for WPA2 Enterprise Enabled SSIDs** The supported methods are **EAP-FAST**, **PEAP-MSCHAPv2**, and **EAP-TLS**. If you select EAP-TLS, a certificate and its password are required. You can upload a certificate by clicking the **Certificate** drop-down menu and then clicking **Add New Certificate Bundle**.

Setting	Description
Interval drop-down menu	Specify the schedule for the sensor test. Options are: • **Daily**: The sensor test occurs on an ongoing recurring interval. The default interval is every hour. • **Once**: The sensor test occurs one time at a specified date and time.

Step 5 Click **Next** to continue to the **Select Tests** step.

Step 6 For the **Select Tests** step, configure the following settings:

a) Check the check boxes for the **Network Tests** that you want to run, and then enter the required information for those tests:

Networking Tests	
Test Type	**Description**
Onboarding Tests	Performs a client onboarding test that typically involves association, AAA, and DHCP. **Note** • This option is selected by default and cannot be unselected. • **Onboarding Tests** is supported on Cisco Aironet 1800s Active Sensors with Software Release 8.8.260.0 and later.
DNS Tests	Resolves IP address for the domain name.
Host Reachability Tests	Verifies reachability using the Internet Control Message Protocol (ICMP) echo request.
RADIUS Tests	The sensor acts as a Dot1x supplicant and authenticates through wireless. Dot1x supplicant supports protocols such as Protected Extensible Authentication Protocol (PEAP) with Password Authentication Protocol (PAP) or the Microsoft version of the Challenge-Handshake Authentication Protocol (MS-CHAP).

b) Check the check boxes for the **Performance Tests** that you want to run, and then enter the required information for those tests:

Performance Tests	
Test Type	**Description**
Speed Test	If you have a Network Diagnostics Test (NDT) server, enter the IP address of the NTD server in the field provided. If the NDT server is reachable through a proxy server, enter the IP address of the proxy server in the field provided.
IPSLA Test	Runs UDP jitter, UDP echo, packet loss, and latency measurements from the sensor to APs. To run the IPSLA test, choose a **Service Level** option for each SSID from the drop-down list. Options are **Platinum** (voice), **Gold** (video), **Silver** (best effort), and **Bronze** (background).

| Note | Speed Test and IPSLA Test are supported on Cisco Wireless Controllers and Cisco Aironet 1800s Active Sensors with Software Release 8.8 and later. |

c) Check the check boxes for the **Application Tests** that you want to run, and then enter the required information for those tests:

Email Tests	
Test Type	**Description**
Email Tests	Includes the following: • **POP3**: Post Office Protocol3, connects to POP3 server TCP port (110). • **IMAP**: Internet Message Access Protocol, connects to IMAP server TCP port (143). • **Outlook Web Server**: Logs into the Outlook Web Server (OWS) and verifies access.
Web Tests	Tests for access to the provided URL and verification of the response data.
File Transfer Tests	Tests for file upload and download operations. Note The maximum file size for the sensor test is 5 MB.

Step 7   Click **Next** to continue to the **Select Sensors** step.

Step 8   For the **Select Tests** step, configure the following settings:

• To set the RSSI threshold value for all APs, do the following:

   a. Click **Thresholds** and drag the **RSSI Threshold** slider to the desired value.

   b. From the **Number of Target APs** drop-down list, choose the number of APs you want the sensor to test against.

   c. Click **Apply**.

• To select specific APs to test, do the following:

   a. Check the check boxes of the sensors you want to use for the test.

   b. Click ˇ in the **Target AP #** column to view the all sensor neighboring APs.

   c. Check the check boxes of the desired APs to test in the **Target AP** column.

   | Note | • You can choose a maximum number of five APs.

• The sensor's neighboring APs are updated every 30 minutes. |

Step 9   Click **Next** to create the sensor test.

The new test is added and appears on the **Test Suites** window.

Create and Run Sensor-Driven Tests Using Templates

Use this procedure to create and run sensor-driven tests using templates. The workflow for sensor-driven tests using templates consists of two parts:

1. **Create the test template**: Configure the test configurations such as the SSIDs to test, test types to use, and the AP coverage.

2. **Deploy the test template**: After a test template is created, select the locations for testing and set the test schedule. After a test template is deployed, it is ready to be run.

Using templates is beneficial if you have a use case that requires a sensor-driven test to be run at different locations and with different schedules. With templates, you can create duplicates that can be deployed for each instance of the test location and schedule. This saves you time from having to recreate the same test for each instance.

Before you begin

- If you are using the Cisco Aironet 1800s Active Sensor to run sensor-driven tests, make sure that the sensor is provisioned using PnP, so that it displays under **Inventory**. See Provision the Wireless Cisco Aironet 1800s Active Sensor, on page 2.

- Note that if a sensor test template restarts, all sensors on that template begin running their tests at the same time, which causes the result graphs to show a cyclical pattern.

Step 1 From the top-left corner, click the menu icon and choose **Assurance** > **Settings** > **Sensors**.

Step 2 Click the **Test Templates** tab.

The **Test Templates** window appears.

Figure 3: Test Templates Window

Step 3 To create a new sensor test template, click + **Add Sensor Test**.

The wizard for creating a sensor test template appears.

Step 4   For the **Set up Sensor Test** step, configure the following settings:

- **Test Template Name**: Enter the name for the test.

  Note   Use only letters, numbers, underscores, hyphens, and periods.

- **SSID Selection**: Check the check boxes for the SSIDs you want to include for the sensor test.

Step 5   Click **Next**.

Step 6   For the **Enter SSID Credentials** step, enter the credentials for the selected SSIDs:

- For SSIDs with **Open** security, select the following:

  - **Open**: For SSIDs with WebAuth passthrough, enter the email address.

  - **ISE Guest Portal**: Choose the labels for the ISE guest portal.

  - **Clearpass Guest Portal**: Choose the labels for the Clearpass guest portal and then click **Apply**.

- For SSIDs with **WPA2 Personal** security, enter the password.

- For SSIDs with **WPA2 Enterprise** security, enter the EAP method, username, and password.

Step 7   Check the **Add Proxy Settings** check box, to enable proxy settings.

Step 8   Configure the following proxy settings:

- **Proxy Server**

- **Proxy Port**

- **Proxy UserName**

- **Proxy Password**

Step 9   Click **Next**.

Step 10   For the **Define Sensor Test Category Details** step, check the check boxes for the test types to include:

a)   For the **Onboarding** test category, the test types are **Association**, **Authentication**, and **DHCP**.

  Note   All of these test types are selected by default and cannot be excluded from the test template.

b)   For the **RF Assessment** test category, the test types are **Data Rate** and **SNR**.

  Note   All of these test types are selected by default and cannot be excluded from the test template.

c)   For the **Network Services Tests** test category, select from the following test types:

- **DNS**: Resolves IP address for the domain name.

- **RADIUS**: The sensor acts as a Dot1x supplicant and authenticates through wireless.

d)   For the **Performance Tests** test category, select from the following test types:

- **Internet (NDT)**: Performs a speed test using Network Diagnostic Tool (NDT).

If you have a Network Diagnostics Test (NDT) server, enter the IP address of the NTD server in the field provided. If the NDT server is reachable through a proxy server, enter the IP address of the proxy server in the field provided.

- **iPerf3**: iPerf3 test is a tool used to measure network performance. This feature allows you to perform a speed test in the network with a certain amount of traffic to determine whether the test is able to pass through the traffic.

  To run the iPerf3 test, check the iPerf3 check box, and then enter the IP address of the iPerf3 server, UDP bandwidth, and port details in the fields provided.

  iPerf3 Limitations

    - You can add up to five iPerf3 servers.

    - You can configure each iPerf3 server to use a maximum of five ports per template. Sensors randomly select the port in which it wants to run the iPerf3 test.

    - Two sensors cannot connect to the same port concurrently on a given iPerf3 server.

    - The "iPerf: Server Busy" error message indicates that there are not enough iPerf3 instances to support the number of the sensors that are running the iPerf3 test.

      To resolve this issue, do *one* of the following:

        - Add iPerf3 server instances. To do so, expand the ports that support iPerf3 testing on the existing servers.

        - Reduce the number of sensors that are configured to run the iPerf3 test. To do so, create a separate template for iPerf3 testing.

- **IP SLA**: Runs UDP jitter, UDP echo, packet loss, and latency measurements from sensor to APs.

  To run the IPSLA test, choose a **Service Level** option for each SSID from the drop-down list. Options are **Platinum** (voice), **Gold** (video), **Silver** (best effort), and **Bronze** (background).

e) For the **Application Tests** test category, select from the following test types:

- **Host Reachability**: Tests for reachability using (ICMP) echo request.

- **Web**: Tests for access to the provided URL and verification of the response data.

- **FTP**: Tests for file upload and download operations

  Note   The maximum file size for the sensor test is 5 MB.

f) For the **Email** test category, select from the following test types:

- **POP3**: Post Office Protocol3, connects to POP3 server TCP port (110).

- **IMAP**: Internet Message Access Protocol, connects to IMAP server TCP port (143).

- **Outlook Web Access**: Logs into the Outlook Web Server (OWS) and verifies access.

Step 11   Click **Next**.

Step 12   For the **Select AP Coverage** step, do the following:

a) Select the frequency bands to test with the **2.4GHz** and **5GHz** check boxes.

      b) In the **Number of Target APs** drop-list for the selected bands, choose the number of APs you want the sensor to test against.

          Note   You can choose a maximum of five APs.

      c) In the **RSSI Range** slider for the selected bands, drag the slider to the desired RSSI.

Step 13   Click **Next**.

Step 14   For the **Summary** step, review the template settings.

             Click **Edit** for the **SSIDs** or **AP Coverage** steps to reconfigure its settings.

Step 15   Click **Create Test** to create the template.
The test template is created and a dialog box appears for confirmation.

Step 16   For the **Done! Sensor Test Created** confirmation window, click **Deploy Test to Locations** to configure the locations and schedule for the test template.

          Important   If you return to the **Test Templates** window without deploying the test, click **Deploy Test** from the **Location** column to continue to the next step of deploying the test.

Step 17   For the **Select Location** step, use the hierarchy menu on the left to check the check boxes for the sites, buildings, or locations that you want to deploy the test template.

Step 18   Click **Next**.

Step 19   For the **Set Schedule** step, select from one of the options for the test frequency:

      • **Periodic**: Runs the test at specified intervals. Use the **Interval** drop-down list to select the time between intervals.

      • **Scheduled**: Runs the tests on designated days of the weeks for a specified duration:

          a. Click the **S**, **M**, **T**, **W**, **T**, **F**, and **S** buttons to select the days of the week to run the test.

          b. For selected days, specify the start and end time for the test period from the **From** time pickers.

          c. In the **Select Value** drop-down menu, select the desired test duration for the test period.

          d. To add another test period for the selected day, click + **Add** to add a new row for configuring the test period.

          e. To remove a test period, click the trash can icon.

      • **Continuous**: The test runs indefinitely and repeats after completion.

Step 20   Click **Next**.

Step 21   For the **Summary** step, review the deployment details.

             Click **Edit** for the **Location** or **Schedule** steps to reconfigure its settings.

Step 22   Click **Deploy Test**.
The test template appears in the **Test Template** window.

Step 23   Click **Run Now** for the test template to run the test.

Manage Sensor-Driven Test Templates

Use this procedure to manage sensor-driven test templates. You can duplicate and delete sensor-driven test templates, as well as undeploy running sensor-driven test templates.

Before you begin

Create sensor-driven test templates. See Create and Run Sensor-Driven Tests Using Templates, on page 22.

Step 1   From the top-left corner, click the menu icon and choose **Assurance** > **Settings** > **Sensors**.

Step 2   Click the **Test Templates** tab.

The **Test Templates** window appears.

Figure 4: Test Templates Window

Step 3   To duplicate a test template, do the following:

a)   Check the check box for the test template you want to duplicate.

b)   Choose **Actions** > **Duplicate**.

c)   In the **Input the new Test Name** dialog box, enter the name for the duplicate of test template.

d)   Click **Save**.
The duplicate of the test template appears in the **Test Templates** window. To deploy the test, click **Deploy Test** from the **Location** step.

Step 4   To delete a test template, do the following:

a)   Check the check box for the test template you want to duplicate.

b)   Choose **Actions** > **Delete**.

c)   In the **Warning** dialog box, click **Yes**.
The test template is deleted.

Step 5   To undeploy a test template, do the following:

a)   Check the check box for the running test template you want to undeploy.

b)   Choose **Actions** > **Undeploy**.

c) In the **Warning** dialog box, click **Yes**.
The test template stops running.

| Warning | If you undeploy a test template, its location and schedule settings are removed. |