



# Manage Sensors and Sensor-Driven Tests

---

- [About sensors and sensor-driven tests, on page 1](#)
- [Provision sensors, on page 1](#)
- [Monitor and troubleshoot network health with sensors, on page 6](#)
- [Manage sensors and backhaul settings, on page 13](#)
- [Manage SCEP profiles, on page 17](#)
- [Sensor-driven tests, on page 18](#)

## 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 doing 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.

## Provision sensors

### Provision the wireless Cisco Aironet 1800s Active Sensor

#### Procedure

---

**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 select the sensor device profile `CiscoProvisioningSSID`. Instead, select 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 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 an AP or sensor device, on page 4](#).
- Step 4** (Optional) After the sensor device is available in the device inventory, you can select to upgrade the software image. See the "Provision Software Images" topic in the *Cisco Catalyst Center User Guide*.
- 

## Enable Provisioning SSID on the wireless controller

### Procedure

---

- 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, select **Open**.
- Step 7** From the **Provisioning** drop-down list, select **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 Catalyst Center IP address, which is done using DHCP Option 43 or through DNS.

---

# Enable Provisioning SSID on the Cisco Catalyst Wireless Controller

## Procedure

---

- 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 these steps:
- From the **Network Assurance Configuration** area, set the **Service Status** toggle to **Enabled**.
  - 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.  
This 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 done.
- Step 6** Verify that the **CiscoSensorProvisioning** policy profile is created.
- From the left-navigation pane, choose **Configuration > Policy**.  
The **Policy Profile** page appears.
  - 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 these steps:
- From the left-navigation pane, choose **Configuration > Tags**.  
The **Manage Tags** page appears.
  - In the **Policy** tab, click **Add**.
  - In the **Name** field, enter a unique name for the Policy Tag.
  - Click **Add**.
  - From the **WLAN Profile** drop-down list, select **CiscoSensorProvisioning**.
  - From the **Policy Profile** drop-down list, select **CiscoSensorProvisioning**.
  - Click ✓.
  - 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 an AP or sensor device

Use this procedure to claim an AP or sensor 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, check the device clean-up and reset details in the [Network Plug and Play Troubleshooting Guide](#).
- For APs in intent-based networks, define the site within the network hierarchy. Refer to [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.

- For provisioning a sensor device, ensure that the sensor is reachable through the Catalyst Center enterprise IP address (private/enp9s0). A DHCP option 43 string makes the device reachable in unclaimed mode in Catalyst 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 Catalyst Center associated with the enp9s0 interface.

### Procedure

**Step 1** Navigate to the **Plug and Play** to choose the required devices.

- From the main menu, choose **Provision > Plug and Play**.
- View the devices in the table.

You can use the search bar to find specific devices.

- Check the check box next to the devices that you want to claim.
- From the menu bar above the device table, choose **Actions > Claim**.

**Step 2** (Optional) In the **Assign Site** window, do these steps:

- Change the device hostname, if needed.
- Assign a site by doing any of these tasks:
  - To assign a different site to each device, click **Assign**, and from the **Select a Site** drop-down list, select 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 select **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 select **Assign this Site to Other Devices**, select 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, Catalyst 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, **Configure APs** assigns this site as the AP location during PnP onboarding.
- If the **Configure AP Location** check box is unchecked, Catalyst 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, refer to "Configure AP location for PnP onboarding" in the *Cisco Catalyst Center Administrator Guide*.

- c) Click **Next**.

**Step 3**

In the **Assign Configuration** window, do these steps:

- 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 continue to the next step. Otherwise, change or configure any of these settings:

- **Device Name:** Change the device hostname, if needed.
- **Template:** From this drop-down list, select 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. The template that you choose must include the CLI commands necessary to configure the global device credentials on the device. Otherwise, the device is added to the inventory in an unmanaged state.

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

**Note**

For Cisco Aironet 1800s Active Sensor earlier than 1.3.1.2, make sure that you do not select the sensor device profile **CiscoProvisioningSSID**. Instead, select 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, select any these options:

- **Clear Device Certificates:** Select this option and check the check box next to each of the devices that you want to clear the certificate from, and click **Clear**.
- **Clear Images:** Select this option and check the check box next to each of the devices that you want to clear the image from, and click **Clear**.
- **Clear Templates:** Select this option and check the check box next to each of the devices that you want to clear the template from, and click **Clear**.

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

- To apply an image or template from one device to other devices, in the **Actions** column, hover your cursor over the ellipsis icon **...** and select **Apply Image to Other Devices** or **Apply Template to Other Devices**.
- 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.
- After you have configured all the devices, click **Next**.

**Step 4** In the **Provision Templates** window, select the template from the **Devices** area, enter your domain name in the **domain** field, and click **Next**.

**Note**

If device is assigned to a site, click **Next**.

**Step 5** In the **Summary** window, view details about the devices and their configuration preview.

**Step 6** Check the **Device Configuration** column for each device to verify if the configuration preview succeeded.

If the preview shows an error, you can click the **Actions** link in the error message above the table to verify 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 device is assigned.

**Step 7** In the **Device Configuration** column, click **Preview Configuration** to review the configuration.

**Step 8** Click **Claim**.

**Step 9** 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 continue 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, refer to the "Complete the provisioning process" in the [Cisco Catalyst 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.

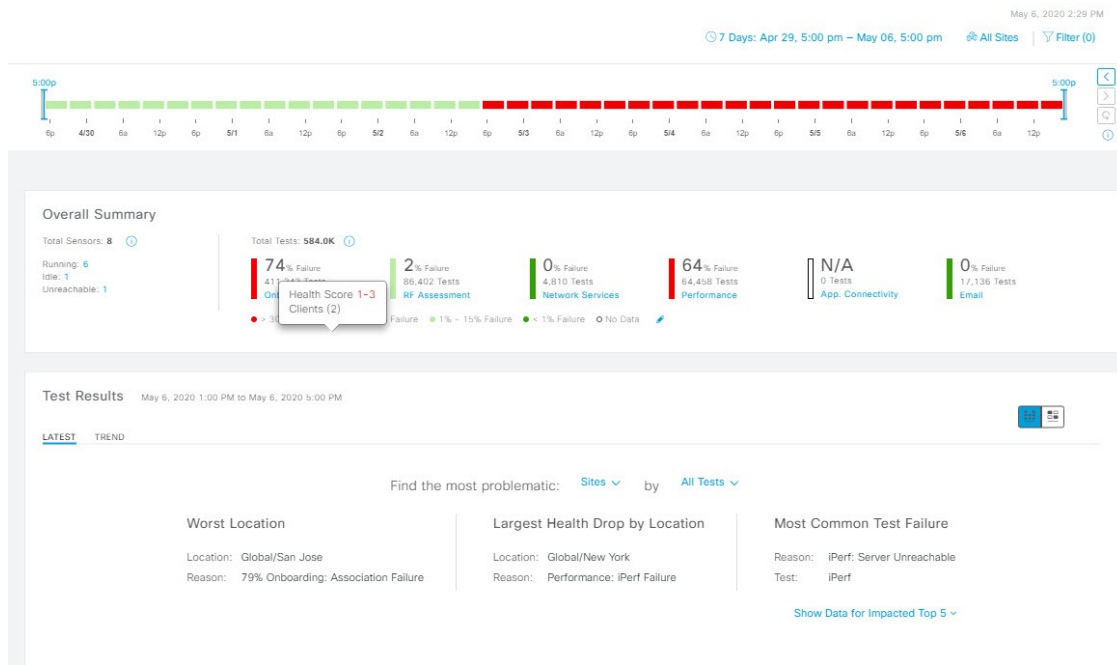
**Before you begin**

Make sure you have added and scheduled sensor-driven tests. See [Create and run sensor-driven tests using templates, on page 18](#).


**Procedure**


**Step 1** From the main menu, choose **Assurance > Dashboards > Wireless Sensors**.

*Figure 1: Wireless sensors dashboard*




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

Timeline area	
Item	Description
 <b>Time Range</b> setting	Enables you to display data within a specified time range on the dashboard. Do these steps: <ol style="list-style-type: none"> <li>From the drop-down menu, select the length of the range: <b>3 Hours</b>, <b>24 Hours</b>, or <b>7 Days</b>.</li> <li>Specify the <b>Start Date</b> and time; and the <b>End Date</b> and time.</li> <li>Click <b>Apply</b>.</li> </ol>

Timeline area	
Item	Description
 <b>Hierarchy Location</b> setting	<p>Enables you to select 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.</p> <p><b>Note</b> 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.</p>
<b>Filter</b> icon	<p>Enables you to select the data displayed on the dashboard based on SSIDs and radio frequency bands.</p> <p>To add filters:</p> <ol style="list-style-type: none"> <li>Click <b>Filter</b>.</li> <li>From the drop-down menu, click the <b>SSID</b> tab and check the check boxes for the desired SSIDs.</li> <li>From the drop-down menu, click the <b>Band</b> tab and select the radio button for <b>2.4 GHz</b> or <b>5 GHz</b>.</li> <li>Click <b>Apply</b>.</li> </ol> <p>To remove all selected filters:</p> <ol style="list-style-type: none"> <li>Click the <b>Filter</b> icon.</li> <li>Click <b>Clear Filters</b>.</li> </ol>

**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 this functionality:

Overall summary dashlet	
Item	Description
<b>Total Sensors</b> area	<p>Provides an overall view of all the sensors in your network and their status. The status types of the sensor include:</p> <ul style="list-style-type: none"> <li>• <b>Idle</b>: The sensor is onboarded and does not have any scheduled tests.</li> <li>• <b>Running</b>: The sensor is onboarded and is included in a test suite or test template.</li> <li>• <b>Unreachable</b>: No heartbeat received from the sensor.</li> </ul> <p>Click the hyperlinked number next to the status type to open a slide-in pane that displays the sensors with that status.</p> <p>In the slide-in pane, you can click the sensor name under the <b>Name</b> column to get a 360° view of that sensor. See <a href="#">Monitor and troubleshoot network health with a wireless sensor, on page 11</a>.</p>
<b>Total Tests</b>	<p>Displays the total number of tests performed by all sensors and a breakdown of the test results based on these test categories:</p> <ul style="list-style-type: none"> <li><b>Onboarding</b></li> <li><b>RF Assessment</b></li> <li><b>Network Services</b></li> <li><b>Performance</b></li> <li><b>App. Connectivity</b></li> <li><b>Email</b></li> </ul> <p>You can click a test category to open a slide-in pane with additional details about its test results.</p> <p>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:</p> <ul style="list-style-type: none"> <li>• A chart that displays the test results, future trends, and list of APs used in the tests.</li> </ul> <p><b>Note</b> For the <b>RF Assessment</b> test category, the chart displays the KPIs data rate and SNR, instead of test results.</p> <ul style="list-style-type: none"> <li>• Data type categories: <b>Top Failure Reasons</b> (if applicable), <b>Top APs</b>, <b>Top Locations</b>, <b>Top Bands</b>, and <b>Top SSIDs</b> (if applicable).</li> <li>• A table with detailed data of the sensors that ran the tests.</li> </ul> <p>You can click the data segments from the data type categories to filter the data that appears in the table.</p>

Overall summary dashlet	
Item	Description
 <b>Edit Threshold</b>	<p>Enables you to customize the thresholds of the color-coded ranges that indicate the severity of percentage of test result failures.</p> <p>  &gt; 30% Failure            15% - 30% Failure            1% - 15% Failure            &lt; 1% Failure         </p> <p>To customize the thresholds:</p> <ol style="list-style-type: none"> <li>Click the edit () icon.</li> <li>In the <b>Edit Threshold</b> menu, enter the percentage values in the fields for each color-coded range.</li> <li>Click <b>Apply</b>.</li> </ol>

**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
<b>Latest</b> tab and <b>Trend</b> tab	<p>These tabs determine the scope of the data that is displayed in the dashlet:</p> <ul style="list-style-type: none"> <li>• <b>Latest</b>: Displays the data from the selected time window in the timeline on the top of the window.</li> <li>• <b>Trend</b>: Displays data from the last 24 hours.</li> </ul>
 <b>Heatmap View</b> and <b>Card View</b> toggle	<p>This toggle button allows you to change the view of the dashlet to the <b>Heatmap View</b> and the <b>Card View</b>.</p> <p>The <b>Heatmap View</b> is displayed by default.</p>

Test results dashlet	
Item	Description
 <b>Heatmap View</b>	<p>Displays the top 5 rankings of these statistical categories at the top of the dashlet:</p> <ul style="list-style-type: none"> <li>• <b>Worst Location, Buildings, Floors, or Sensors:</b> Sites, buildings, floors, or sensors with the highest test result failure percentage.</li> <li>• <b>Largest Health Drop by Location, Buildings, Floors, or Sensors:</b> Sites, buildings, floors, or sensors with the largest sudden drop.</li> <li>• <b>Most Common Test Failure:</b> Test types that had the highest test result failures.</li> </ul> <p>Only the top spot for each statistical category is displayed. Click <b>Show Data for Impact Top 5</b> to see the complete rankings.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• Use the drop-down lists in the <b>Find the most problematic</b> 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.</li> <li>• Use the search field to filter the heatmap for specific locations or sensors.</li> <li>• Hover your cursor over a block to view the exact percentage value for test result failures.</li> <li>• Click a color-coded block to open a slide-in pane with further details about the test results at that intersect.</li> </ul>
 <b>Card View</b>	<p>Displays the data in a card format for high-level monitoring and comparison.</p> <p>Use the drop-down lists in the <b>Find the most problematic</b> area to sort the data.</p>

## 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.

### Procedure

- Step 1** From the main menu, choose **Assurance > Dashboards > Wireless Sensors**.  
The **Sensor Dashboard** appears.
- Step 2** From the **Sensors Dashboard**, do one of these tasks:
- 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:

- From the drop-down menu, select a time range: **3 hours**, **24 hours**, or **7 days**.
- Specify the Start date and time; and the End date and time.
- 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:


- Click **View Logs** at the end of the header.  
The **Event Logs** slide-in pane appears which displays the event logs.
- 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.

- 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 this 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, the status LED, and change the name for these sensors.

**Before you begin**

Make sure the sensors are assigned to a site.

**Procedure**

**Step 1** From the main menu, choose **Assurance > Settings > Sensors**.

The **Sensor List** window appears.

Figure 2: Sensor List window


Sensor	Status	SSH	LED	Location	SCEP Profile	Last Seen	Backhaul Type
wired4540	Running	On	On	.../New York/ny-bld-1/ny-floor-1	MS	May 6, 2020 2:48 pm	Wired
AP70F3.5A88.4DB0	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	ISE51	May 6, 2020 2:48 pm	Wireless
AP70F3.5A80.6300	Running	Off	On	.../New York/ny-bld-1/ny-floor-1	MS	May 6, 2020 2:48 pm	Wireless
AP70F3.5A80.2088	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	ISE52	May 6, 2020 2:48 pm	Wired
AP70F3.5A7E.3BC0	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	MS	May 6, 2020 2:48 pm	Wireless
AP70F3.5A7E.26C0	Running	On	On	...an Jose/sjc-bld-1/sjc-floor-1	MS	May 6, 2020 2:48 pm	Wired
60C8wireless	Idle	On	On	...ngalore/big-bld-1/big-floor-1	None	May 6, 2020 2:48 pm	Wireless
5FE0wireless	Idle	On	On	...ngalore/big-bld-1/big-floor-1	ISE52	May 6, 2020 2:48 pm	Wireless

**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 their 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.

**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:

- a) Check the check box of the sensor.
- b) Hover your cursor over the **Actions** drop-down list and select **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:

- a) Check the check box of the sensor.
- b) Hover your cursor over the **Actions** drop-down list and select **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:

- a) Check the check box of the sensor.
- b) From the **Actions** drop-down list, select **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:

- a) Check the check box of the sensor.
- b) From the **Actions** drop-down list, select **Enroll using SCEP**.  
The **Enroll using SCEP** slide-in pane appears.
- c) Select 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 select 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 Catalyst Center.

For information about a persistent wireless backhaul connection, see [Persistent wireless backhaul connections on sensor devices, on page 17](#).

### Procedure

---

**Step 1** From the main menu, choose **Assurance > Settings > Sensors**.

The **Sensor List** window appears.

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

**Step 3** You can add and manage backhaul SSIDs by doing these steps:

- 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, do this configuration:

- **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 select **802.1x EAP**, you must select one of these 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:** Select **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.  
If you select **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:** Select **Enroll Using Certificate Bundle** or **Enroll Using SCEP**.  
If you select **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 do this configuration.

- **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 these steps:

- a) Check the check box of the backhaul configuration.
- b) Hover your cursor over the **Actions** drop-down list and select **Edit**.

**Step 5** You can delete a backhaul configuration by doing these steps:

- a) Check the check box of the backhaul configuration.
- b) Hover your cursor over the **Actions** drop-down list and select **Delete**.

## Persistent wireless backhaul connections on sensor devices

Catalyst 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 these 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.

### Procedure

---

**Step 1** From the main menu, choose **Assurance > Settings > Sensors**.

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

**Step 3** To add and manage an SCEP profile:

a) Click **Add SCEP Profiles**.

The **Create SCEP Profile** window appears.

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

- **SCEP Profile Name:** Enter a name for the SCEP profile.
- **URL Base:** Enter a valid server.

**Note**

For **ISE**, enter this information:

**http://ISE\_IP\_or\_FQDN\_Name:9090/auth/caservice/pkclient.exe**

For **Microsoft CA**, enter this information:

**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:

- a) Check the check box next to the SCEP profile.
- b) From the **Actions** drop-down list, select **Edit**.

**Step 5** To delete a SCEP profile:

- a) Check the check box next to the SCEP Profile.
- b) From the **Actions** drop-down list, select **Delete**.

---

## Sensor-driven tests

### 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 1](#).
- 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.

## Procedure

**Step 1** From the main menu, choose **Assurance > Sensors**.

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

The **Test Templates** window appears.

**Figure 3: Test Templates window**

Test Name	SSID with Test Types	AP Coverage	Location	Schedule
<input type="checkbox"/> sjcdot1x	5520-LOCAL-WLAN-1: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bld-1/sjc-floor-1	Continuous <span>Run Now</span>
<input type="checkbox"/> EAPTLS	ISEEAPTLS: Onboarding, RF Assessment, App.Connectivity, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bld-1/sjc-floor-1	Continuous <span>Run Now</span>
<input type="checkbox"/> 3rd party test	8540-hidden: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bld-1/sjc-floor-1	Continuous <span>Run Now</span>
<input type="checkbox"/> NYC	SensorSSID: Onboarding, RF Assessment, Net.Service, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/New York/ny-bld-1/ny-floor-1	Periodic <span>Run Now</span>
<input type="checkbox"/> EAPTLS8540	EAPTLS8540: Onboarding, RF Assessment	5GHz: 1, -70dBm	Deploy Test	N/A

Showing 5 of 5

**Step 3** Click + **Add Sensor Test** to create a new sensor test template.

The workflow for creating a sensor test template appears.

**Step 4** On the **Set up Sensor Test** window, configure these 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** On the **Enter SSID Credentials** window, enter the credentials for the selected SSIDs:

- For SSIDs with **Open** security, select these options:
  - **Open:** For SSIDs with WebAuth passthrough, enter the email address.
  - **ISE Guest Portal:** Select the labels for the ISE guest portal.
  - **Clearpass Guest Portal:** Select 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 6**

To enable proxy settings:

- a. Check the **Add Proxy Settings** check box.
- b. Configure these proxy settings:
  - **Proxy Server**
  - **Proxy Port**
  - **Proxy UserName**
  - **Proxy Password**

**Step 7**

On the **Define Sensor Test Category Details** window, check the check boxes for the tests that you want 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 these test types:

- **DNS**: Resolves the 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 these test types:

- **Internet (NDT)**: Does 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 these tasks:

- 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 IP SLA test, select 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 these 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 these 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 8**

On the **Select AP Coverage** window, do these steps:

- a) Check the frequency band check boxes (**2.4GHz** and **5GHz**) that you want to test.
- b) From the **Number of Target APs** drop-list for the selected bands, select the number of APs that you want the sensor to test against.

**Note**

You can select a maximum of five APs.

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

**Step 9**

On the **Summary** window, review the template settings.

To reconfigure the settings, click **Edit** in the **SSIDs** and **AP Coverage** dashlets.

**Step 10**

Click **Create Test** to create the template.

The test template is created and a dialog box appears for confirmation.

**Step 11**

On 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 12**

On the **Select Location** window, from the left tree hierarchy, check the check boxes of the sites where you want to deploy the test template.

- Step 13** On the **Set Schedule** window, select one of the test frequency options:
- **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 the selected days, specify the start and end time for the test period from the **From** time pickers.
    - c. From 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 14** On the **Summary** window, review the deployment details.  
To update the details, click **Edit** in the **Location** and **Schedule** dashlets.
- Step 15** Click **Deploy Test**.  
If you plan to run IP SLA performance tests, the **Warning** dialog box appears. Click **Deploy** to confirm that you want to enable IP SLA on the wireless controllers in the selected sites, so the sensors can run IP SLA tests against the APs.  
The test template displays in the **Test Templates** table on the **Test Templates** window.
- Step 16** Click the test template's corresponding **Run Now** 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 18](#).

### Procedure

---

- Step 1** From the main menu, choose **Assurance > Sensors**.
- Step 2** Click the **Test Templates** tab.  
The **Test Templates** window appears.

Figure 4: Test Templates window

Sensor List		Test Templates	Legacy Tests	Setting		
Actions					Last updated: 2:48 PM	EQ Find
<input type="checkbox"/>	Test Name	SSID with Test Types	AP Coverage	Location	Schedule	
<input type="checkbox"/>	sjcdot1x	5520-LOCAL-WLAN-1: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bid-1/sjc-floor-1	Continuous	Run Now
<input type="checkbox"/>	EAPTLS	ISEEAPTLS: Onboarding, RF Assessment, App.Connectivity, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bid-1/sjc-floor-1	Continuous	Run Now
<input type="checkbox"/>	3rd party test	8540-hidden: Onboarding, RF Assessment, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/San Jose/sjc-bid-1/sjc-floor-1	Continuous	Run Now
<input type="checkbox"/>	NYC	SensorSSID: Onboarding, RF Assessment, Net.Service, Performance	2.4GHz: 1, -70dBm 5GHz: 1, -70dBm	Global/New York/ny-bid-1/ny-floor-1	Periodic	Run Now
<input type="checkbox"/>	EAPTLS8540	EAPTLS8540: Onboarding, RF Assessment	5GHz: 1, -70dBm	Deploy Test	N/A	

Showing 5 of 5

**Step 3** To duplicate a test template:

- Check the check box for the test template that you want to duplicate.
- From the **Actions** drop-down list, select **Duplicate**.
- In the **Input the new Test Name** dialog box, enter a name for the duplicate test template.
- Click **Save**.

The duplicate of the test template displays in the **Test Templates** window. To deploy the test, click the test template's corresponding **Deploy Test** from the **Location** column.

**Step 4** To delete a test template:

- Check the check box for the test template that you want to delete.
- From the **Actions** drop-down list, select **Delete**.
- In the **Warning** dialog box, click **Yes**.  
The test template is deleted.

**Step 5** To undeploy a test template:

- Check the check box for the running test template that you want to undeploy.
- From the **Actions** drop-down list, select **Undeploy**.
- In the **Warning** dialog box, click **Undeploy**.

**Note**

If the test template is configured to run IP SLA performance tests, clicking **Undeploy** confirms that you want to disable IP SLA on the wireless controllers in the selected sites, so the sensors don't run IP SLA tests against the APs.

The test template stops running.

**Warning**

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

