Manage Intelligent Capture

About Intelligent Capture

For Catalyst Center, all information about device and client health is typically available from Cisco wireless controllers. Intelligent Capture provides support for a direct communication link between Catalyst Center and access points (APs), so each of the APs can communicate with Catalyst Center directly. Using this channel, Catalyst Center can receive packet capture data, AP and client statistics, and spectrum data. With the direct communication link between Catalyst Center and APs, Intelligent Capture allows you to access data from APs that is not available from wireless controllers.

Note

- Intelligent Capture is only supported for APs in either local or FlexConnect mode.
- Intelligent Capture is not supported in SDA deployments.

Supported Devices for Intelligent Capture

The following table lists the Cisco Wireless Controllers that support Intelligent Capture:

Table 1: Supported Cisco Wireless Controllers

Supported Cisco Wireless Controllers	
Device	**Minimum Supported Software Version**
Cisco 3504 Wireless Controller	AireOS 8.8.125.0
Cisco 5520 Wireless Controller	AireOS 8.8.125.0
Cisco 8540 Wireless Controller	AireOS 8.8.125.0

The following table lists the Cisco Catalyst Wireless Controllers that support Intelligent Capture:

Table 2: Supported Cisco Catalyst Wireless Controllers

Supported Cisco Catalyst Wireless Controllers	
Device	**Minimum Supported Software Version**
Cisco Catalyst 9800 Series Wireless Controllers	IOS-XE 16.12.1.s

The following table lists the Cisco APs that support Intelligent Capture:

Table 3: Cisco APs support for Intelligent Capture

Supported Cisco APs			Intelligent Capture Feature Support			
Device	**Minimum Supported AireOS Software Version**	**Minimum Supported IOS-XE Software Version**	**Anomaly Packet Capture**	**Live/ Scheduled Packet Capture**	**Full Packet Capture**	**Spectrum Analysis**
Aironet 1540 APs[1]	8.10.105.0	16.12.1.s	Yes	Yes	No	No
Aironet 1560 APs	8.10.105.0	16.12.1s	Yes	Yes	No	Yes
Aironet 1815 APs[1]	8.10.105.0	16.12.1s	Yes	Yes	No	No
Aironet 1830 APs[1]	8.10.105.0	16.12.1s	Yes	Yes	No	No
Aironet 1840 APs[1]	8.10.105.0	16.12.1s	Yes	Yes	No	No
Aironet 1850 APs[1]	8.10.105.0	16.12.1s	Yes	Yes	No	No
Aironet 2800 Series AP	8.8.125.0 or 8.10	16.12.1s	Yes	Yes	No	Yes

Supported Cisco APs			Intelligent Capture Feature Support			
Device	**Minimum Supported AireOS Software Version**	**Minimum Supported IOS-XE Software Version**	**Anomaly Packet Capture**	**Live/ Scheduled Packet Capture**	**Full Packet Capture**	**Spectrum Analysis**
Aironet 3800 Series APs	8.8.125.0 or 8.10	16.12.1s	Yes	Yes	No	Yes
Aironet 4800 Series APs[2]	8.8.125.0 or 8.10	16.12.1s	Yes	Yes	Yes	Yes
Catalyst 9105 AP[1]	8.10 MR3	17.3.1	Yes	Yes	No	No
Catalyst 9115 AP[1]	8.10.105.0	16.12.1s	Yes	Yes	No	Yes
Catalyst 9120 AP	8.10.105.0 8.10.112.0 (for Spectrum Analysis)	16.12.1s 17.2.1 (for Spectrum Analysis)	Yes	Yes	No	Yes (from 17.2.1)
Catalyst 9130 AP[2]	8.10 MR3	17.3.1	Yes	Yes	Yes	Yes
Catalyst IW6300 Heavy Duty Series APs	8.10.105.0	17.1.1s	Yes	Yes	No	Yes
Catalyst ESW6300 Embedded Services APs	8.10.105.0	17.1.1s	Yes	Yes	No	Yes
Catalyst Wireless 9162 APs	NA	17.9.2	Yes	Yes	No	Yes
Catalyst Wireless 9164 APs	NA	17.9.1	Yes	Yes	No	Yes
Catalyst Wireless 9166 APs	NA	17.9.1	Yes	Yes	Yes	Yes
Catalyst 9136 Series APs	NA	17.7.1	Yes	Yes	Yes	Yes

[1] Spectrum Analysis is *not supported* on the following APs: Aironet 1540 AP, Aironet 1800 Series APs, Catalyst 9105 AP.

[2] Data Packet Capture and Full Packet Capture is only supported on Aironet 4800 APs and Catalyst 9130 AP, Catalyst 9136 AP, and Catalyst 9166 AP.

Intelligent Capture Best Practices

The following are best practices to ensure Intelligent Capture functions optimally in Catalyst Center:

- After a new wireless controller device is added to Catalyst Center, disable any Intelligent Capture global settings, and then re-enable those settings so that they will be configured on the new wireless controller.
- Before deleting a wireless controller device from Catalyst Center, disable all Intelligent Capture settings.
- Before upgrading any of managed wireless controllers or reimaging Catalyst Center, disable all Intelligent Capture settings, and then re-enable them after completing the upgrade.

Onboarding Packet Capture for a Client Device

About Onboarding Packet Capture for a Client Device

Onboarding Packet Capture sessions capture packets that the client device uses to join a wireless network, such as (802.11 management frames, DHCP, and EAP packets), and collects the client’s RF statistics in 5-second samples. The data is displayed in the **Client 360 > Intelligent Capture** window. The session can be started immediately or scheduled to run later. The default duration of the session is 30 minutes and can be set up to eight hours. By default, Onboarding Packet Capture is enabled on the last client-connected wireless controller. You can select up to three wireless controllers to cover the client roaming scenario.

Note

- "Client Schedule Capture" is now rebranded as “Onboarding Packet Capture”. While streamlining this nomenclature, you may see the former and rebranded names used in different collaterals. However, "Client Schedule Capture" and "Onboarding Packet Capture" refer to the same feature.
- “Live Capture”, "Scheduled Capture", and "Onboarding Packet Capture" all refer to the same feature. These names are used interchangeably throughout different collateral.

Onboarding Packet Capture Session Limitations

Onboarding Packet Capture sessions have the following limitations:

- There are a total of 16 time slots allocated for capture sessions (live and scheduled), where each client in a session uses one time slot and each client can be enabled on up to three wireless controllers.

  If these maximum values are exceeded, for example, you try to start a seventeenth live capture session, an error message is displayed. To schedule another capture session when the maximum time-slot limit is met, you can either stop a running capture session or wait for a capture session to complete. Then you can start a new capture session.

Note The 16-time-slot limit is enforced by the wireless controller.

When capture sessions are configured on Catalyst Center, any live or scheduled capture sessions that Catalyst Center is not aware of (such as partial packet capture sessions that were directly configured on the wireless controller) are removed.

- A maximum of 100 packets involved in onboarding events can be captured during the time period surrounding the event.
- There is a 3.5-GB limit on the total size of all scheduled onboarding packet files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 3.5-GB limit. Additionally, any onboarding packet files that are more than 14 days old are removed, even if the total size limit has not been reached.

About Client Statistics

Onboarding Packet Capture sessions are global settings that enable supported APs to collect client statistics over 5-second intervals.

Client statistics are also collected over 30-second intervals when AP Statistics is enabled for the AP to which the client is connected.

When client statistics are collected, they are displayed on the four RF statistic charts on the **Client 360** > **Intelligent Capture** window.

Run a Live Onboarding Packet Capture Session for a Client Device

Use this procedure to enable a live capture session for a specific client device and view data packets for the onboarding events and RF statistics.

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

The **Overall** health dashboard is displayed.

Step 2 Click the **Client Health** tab.

The **Client Health** window appears.

Step 3 Open the **Client 360** window of a specific client by doing one of the following:

- In the **Client Devices** table, click the hyperlinked identifier or the MAC address of the device.
- In the **Search** field, enter one of the following: user ID (authenticated through Cisco ISE), IP address, or MAC address.

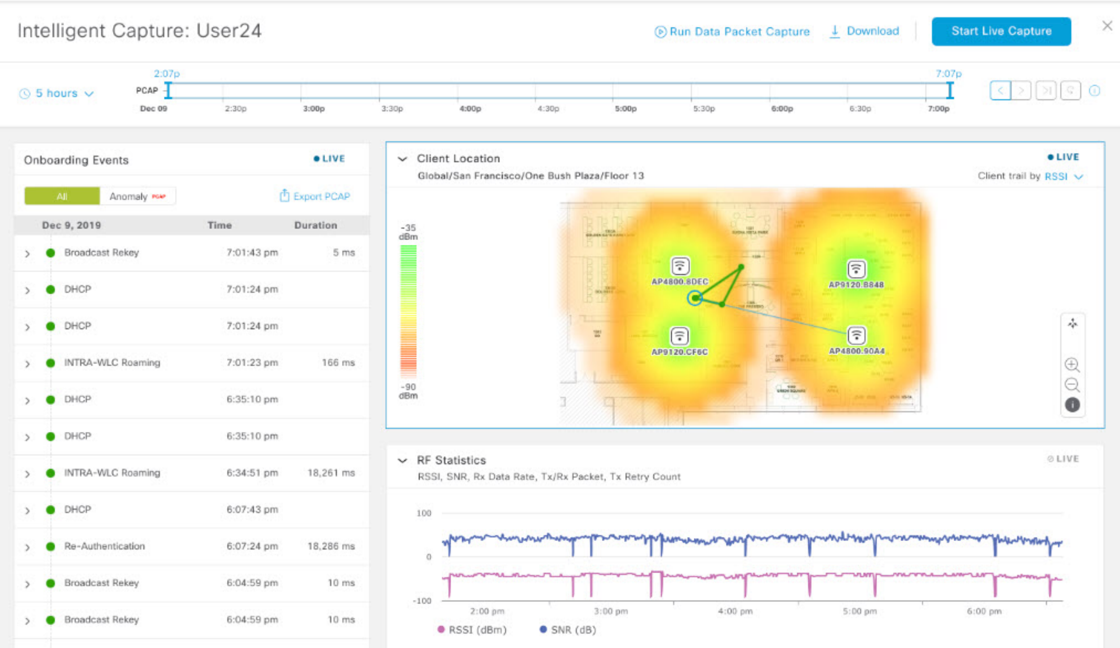
A 360° view of the client device appears.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window appears with the following information:

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or Access Point Unable to Send Intelligent Capture Data to Catalyst Center, on page 37 for more details.

Figure 1: Intelligent Capture Window of a Client



Dec 9, 2019	Time	Duration
Broadcast Rekey	7:01:43 pm	5 ms
DHCP	7:01:24 pm	
DHCP	7:01:24 pm	
INTRA-WLC Roaming	7:01:23 pm	166 ms
DHCP	6:35:10 pm	
DHCP	6:35:10 pm	
INTRA-WLC Roaming	6:34:51 pm	18,261 ms
DHCP	6:07:43 pm	
Re-Authentication	6:07:24 pm	18,286 ms
Broadcast Rekey	6:04:59 pm	10 ms
Broadcast Rekey	6:04:59 pm	10 ms

Step 5 Use the timeline slider for the following functionality:

Timeline Slider

Item	Description
1 hour drop-down list	Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. Default is **1 hour**.
Timeline Slider	The timeline slider determines the time window of all data displayed. A line chart of onboarding events is displayed for the results of a live capture. Green indicates onboarding events and red indicates anomaly events. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. **Note** The timeline can display data from up to two weeks in the past. For more customization of the timeline range, click and drag the boundary lines.

Step 6 To perform a live capture session, do the following:

a) Click **Start Live Capture** at the top-right corner to start a live capture session.

During a live capture session, data packets for the **Onboarding Events** and **RF Statistics** dashlets are collected.

b) Click **Stop Live Capture** to stop the live capture session.

c) View the running live capture sessions in the **Intelligent Capture Settings** window for clients.

Step 7 Use the **Onboarding Events** dashlet to view events that are associated with establishing a network connection:

Onboarding Events Dashlet	
Item	**Description**
All and Anomaly PCAP filter	Allows you to filter the onboarding events. Options are: • **All**: Displays all events. This is the default. • Anomaly PCAP: Filters for only anomaly events that have packets. **Note** If the client has issues joining the network, the word "PCAP" is displayed in red beside the specific event. If the client has no issues joining the network, the word "PCAP" is displayed in gray beside the specific event.
Export PCAP	You can download the packets for a range of specified events: **a.** Click **Export PCAP**. **b.** Specify the first and last events that you want to include in the PCAP. **c.** Click **Download PCAP** to start the download. **Note** Since heuristics are used to determine which packets belong to an event, packets from one minute before the first event and one minute after the last event are included in the download. This ensures that all relevant packets are in the downloaded PCAP. Each export is limited to the first 2000 packets, starting from the oldest timestamp.
List of Onboarding, Incomplete, and Anomaly Events	View the list onboarding, incomplete, and anomaly events in chronological order. Events are color-coded to indicate the following: 🟢: Successful onboarding event. 🔵: Incomplete event. 🔴: Anomaly event. **Note** An event with the word "PCAP" displayed beside it indicates that data packets for this event have been captured for download or analysis. You can click the parent event group to expand it and view the individual events for that group.

Onboarding Events Dashlet	
Item	**Description**
Event Details	You can click an event group or individual event to view the following sections with further details: **Client Location**: Displays the map of the client location and the client's movement during the event. **Auto Packet Analyzer**: This section appears if a live capture, scheduled capture, or anomaly capture session has captured packets for the event. The word "PCAP" that displays next to the event indicates that the event has captured packets. The **Auto Packet Analyzer** section displays a graph with the following information: • The packets (up to 100) surrounding the event are divided into two groups. Gray sections indicate packets that precede the start of an onboarding session. White sections indicate packets in the onboarding session. Deauthentication packets and unexpected patterns of packets are represented by red triangles. These are potentially significant packets that can degrade the client's onboarding experiences. You can download the packets by clicking **Download Packets** for further analysis. • Packet (from client or from AP) • Onboard packet stage identifier • Interpacket gap (ms) • RSSI (dBm) per packet • Associated AP **RF Statistics**: Displays charts with the RF statistic data for the 10-minute interval surrounding the event. The RF statistic data is composed of RSSI and SNR measurements in decibels, Rx average data rate and Rx last data rate, Tx packets and Rx packets, and Tx packet retry. **Note** If Anomaly Capture is enabled, the packets for anomaly events are captured even if a live or scheduled capture is not running.

Step 8 Use the **Client Location** dashlet to view the a floor map with the following information:

- The location of the client and APs on the floor.
- Heatmap with the color intensity representing the strength of the coverage.
- The real-time location of the client on the floor map. If the client moves to another location, its movement is displayed.
- Client trail tracking with color-coded display of connectivity using the RF statistics: RSSI, SNR, data rate, throughput, and packet drop rate.

  The followimg colors on the map indicates the client's health:

  🟢: Good 🟠: Fair 🔴: Poor

- The tracking of the client for a one-minute intervals surrounding the time of the selected onboarding event.
- The replay, stop and start controls below the map can be used to control the viewing.

Note The Client Location feature requires that CMX is integrated with Catalyst Center. For details, see the Integrate Cisco CMX for Wireless Maps chapter.

Step 9 Use the **RF Statistics** dashlet to view detailed RF information.

Four charts that display AP client statistics. For more information, see About Client Statistics, on page 5. The color-coded data contains the following information:

- RSSI and SNR measurements in decibels.
- Rx average data rate (from the past 5 seconds) and Rx last data rate.
- Tx packets and Rx packets.
- Tx packet retry.

You can do the following in the charts:

- Hover your cursor over the chart to see the statistics for a particular time.
- Click and drag within the chart to zoom in on a time period. To change the view to the default, click the 🔍 icon.

Schedule an Onboarding Packet Capture Session for a Client Device

You can schedule an onboarding packet capture session for a client device.

Onboarding Packet Capture sessions collect the following data:

- Data packets for onboarding events and **RF Statistics** chart data (5-second samples) displayed in the **Client 360** > **Intelligent Capture** window. See Run a Live Onboarding Packet Capture Session for a Client Device, on page 5.
- Data for the charts and tables displayed in the **Device 360** > **Intelligent Capture** window. See View RF Statistics of an AP, on page 24 and View Spectrum Analysis Data of an AP, on page 34.

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

The **Onboarding Packet Capture** window is displayed.

Step 2 Click **+ Schedule Client Capture**.

Note If an existing Onboarding Packet Capture task is uncompleted, attempting to start a new packet capture session on the same wireless controllers fails because of the conflicting, uncompleted task. To start a new task, either wait for the existing task to complete or discard it.

Step 3 In the **Schedule Client Capture** slide-in pane, do the following:

a. From the **Select client devices** drop-down list, choose the client devices.

b. From the **Duration** drop-down list, choose the time duration of the Onboarding Packet Capture session.

   The default duration is 30 minutes.

c. Check the check boxes next to the wireless controllers that you want to enable Onboarding Packet Capture on.

   You can choose up to three wireless controllers.

d. Click **Next**.

   All Onboarding Packet Capture sessions are displayed on the **Assurance** > **Intelligent Capture Settings** window in the **Onboarding Packet Capture** tab.

Step 4 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 5 In the **Task Name** field, modify the name if necessary.

Note If the default task name includes "Scheduled Capture", this term refers to Onboarding Packet Capture.

Step 6 Click **Apply**.

Step 7 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 8 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

   For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item’s approval status or the task’s deployment status on the **Tasks** window. If the work item isn’t approved, you need to resubmit the work item for ITSM approval. When it’s approved, it's deployed at the scheduled time.

Note Based on the duration of the task, Catalyst Center automatically runs enable and disable tasks for the Onboarding Packet Capture session. To view the configuration preview of the enable or disable tasks, go to the **Tasks** window, open the task, and click **View Work Item Details**. If you don't view the configuration preview before the task completes, the option to preview will no longer be available.

Stop In-Progress Onboarding Packet Capture Sessions on a Client Device

You can stop an in-progress Onboarding Packet Capture session on a client device.

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

The **Onboarding Packet Capture** window is displayed.

Step 2 Under **In-progress Captures**, check the check boxes next to the wireless controllers that you want to stop running Onboarding Packet Capture sessions on.

Step 3 Click **Stop Capture**.

Full Packet Capture for a Client Device

About Full Packet Capture for a Client Device

Full Packet Capture allows you to capture network data and download the data as PCAP files, which can be viewed in Wireshark. For more information, see Run a Full Packet Capture Session on a Client Device, on page 12.

Note "Client Data Packet Capture" is now rebranded as “Full Packet Capture”. While streamlining this nomenclature, you may see the former and rebranded names used in different collaterals. However, "Client Data Packet Capture" and "Full Packet Capture" refer to the same feature.

Full Packet Capture Limitations

Full Packet Capture has the following limitations:

- Full Packet Capture is supported only on Cisco Aironet 4800 APs and Cisco Catalyst 9130, 9136, and 9166 APs. If Full Packet Capture is enabled and the client roams to an AP that does not support it, full packet capture stops until the client reconnects to an AP that supports full packet capture.
- Only one Full Packet Capture session can run at a time.
- As for all Intelligent Capture features, clocks must be synchronized between Catalyst Center and the Cisco Wireless Controller for Full Packet Capture to work. Ensure that the wireless controller is connected to a Network Time Protocol (NTP) server.
- Each Full Packet Capture session can capture up to 1 GB of rolling data. The 1 GB of data is broken into ten 100-MB files for faster downloads.

Run a Full Packet Capture Session on a Client Device

You can run a Full Packet Capture session on a client device.

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

The **Overall** health dashboard is displayed.

Step 2 Click the **Client Health** tab.

The **Client Health** window is displayed.

Step 3 Open the **Client 360** window of a specific client by doing one of the following:

- In the **Client Devices** table, click the hyperlinked identifier or the MAC address of the device.
- In the **Search** field, enter one of the following: user ID (authenticated through Cisco ISE), IP address, or MAC address.

A 360° view of the client device is displayed.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window is displayed.

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or Access Point Unable to Send Intelligent Capture Data to Catalyst Center, on page 37.

Step 5 Use the timeline slider for the following functionality:

- **1 hour** drop-down list: Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. The default is **1 hour**.

- **Timeline Slider**: The timeline slider determines the time window of all data displayed. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. For more customization of the timeline range, click and drag the boundary lines.

  Note The timeline can display data from up to two weeks in the past.

Step 6 Click **Run Packet Capture**.

The **Run a Data Packet Capture** slide-in pane is displayed, and the **Onboarding Packet Capture** tab is selected by default.

Step 7 In the **Run a Data Packet Capture** slide-in pane, click the **Full Packet Capture** tab.

Note If an existing Full Packet Capture task is uncompleted, attempting to start a new packet capture session on the same wireless controllers fails because of the conflicting, uncompleted task. To start a new task, either wait for the existing task to complete or discard it.

Step 8 From the **Duration** drop-down list, choose the time duration of the packet capture.

The default duration is 30 minutes.

Step 9 Check the check boxes next to the wireless controllers that you want to enable Full Packet Capture on.

You can choose up to three wireless controllers.

Step 10 Click **Next**.

Note

- All Full Packet Capture sessions are displayed under **Assurance** > **Intelligent Capture Settings** > **Full Packet Capture**.
- When a packet capture session is configured on Catalyst Center, any packet capture session that Catalyst Center is not aware of is removed (such as Full Packet Capture sessions that were directly configured on the wireless controller).

Step 11 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 12 In the **Task Name** field, modify the task name if necessary.

Step 13 Click **Apply**.

Step 14 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.

- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 15 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item’s approval status or the task’s deployment status on the **Tasks** window. If the work item isn’t approved, you need to resubmit the work item for ITSM approval. When it’s approved, it's deployed at the scheduled time.

Note Based on the duration of the task, Catalyst Center automatically runs enable and disable tasks for the Full Packet Capture session. To view the configuration preview of the enable or disable tasks, go to the **Tasks** window, open the task, and click **View Work Item Details**. If you don't view the configuration preview before the task completes, the option to preview will no longer be available.

Step 16 To download PCAP files from completed Full Packet Capture and OTA Packet Capture sessions, on the **Intelligent Capture:** *Client Device* window, click **Download**.

You can download files containing information on wireless data, which includes 802.11 files for packets moving between the AP and the client.

Note Data packet captures are divided into separate 100-MB files. There is a 4-GB limit on the total size of all data packet capture files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 4-GB limit. Additionally, any data packet capture files that are more than 14 days old are removed, even if the total size limit has not been reached.

View Full Packet Capture History

Use this procedure to view the history of the full packet capture sessions, such as the time the first packet and the last data packet was captured, the total size of the captured data packets, and the type of packet.

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

The **Onboarding Packet Capture** window is displayed.

Step 2 Click the **Full Packet Capture** tab.

The **Full Packet Capture** window is displayed.

Step 3 Use the **Intelligent Capture Settings - Full Packet Capture** window to view the following information:

Option	Description
Identifier	Displays the client's user ID or hostname. Click the user ID or hostname to open the **Intelligent Capture:** *Client Device* window.
MAC Address	Displays the MAC address of the client device.
Wireless Controller	Displays the name of the wireless controller.
First Packet Time	Displays the time the first data packet was captured.
Last Packet Time	Displays the time the last data packet was captured.
Total Size	Displays the total size of the captured data.
Currently Running	Displays whether the data packet capture is currently running.
Type of Packet	Displays the type of packet, for example, **Wired** or **Wireless**.
Duration	Displays the duration of the packet capture.
Last Start Time	Displays the last started time of the packet capture.
Configuration Status	Displays the configuration status of the devices.

OTA Sniffer Capture for a Wi-Fi Band and Channel

About OTA Sniffer Capture for a Wi-Fi Band and Channel

Catalyst Center allows you to enable OTA Sniffer Capture on a specific radio and bandwidth channel. When it's enabled, all Wi-Fi data packets traveling on the radio and bandwidth channel are captured for download. You can enable up to two APs, where each AP performs radio sniffing on one radio, or enable only one AP to perform network sniffing.

Run an OTA Sniffer Capture Session on a Wi-Fi Band and Channel

You can run an OTA Sniffer Capture session on a Wi-Fi band and channel.

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

The **Overall** health dashboard is displayed.

Step 2 Click the **Client Health** tab.

The **Client Health** window is displayed.

Step 3 Open the **Client 360** window of a specific client by doing one of the following:

- In the **Client Devices** table, click the hyperlinked identifier or the MAC address of the device.
- In the **Search** field, enter one of the following: user ID (authenticated through Cisco ISE), IP address, or MAC address.

Step 4 In the **Client 360** window, click **Intelligent Capture**.

The **Intelligent Capture:** *Client Device* window is displayed.

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** appears next to the client name, see Client or Access Point Unable to Send Intelligent Capture Data to Catalyst Center, on page 37.

Step 5 Use the timeline slider for the following functionality:

- **1 hour** drop-down list: Click the drop-down list and select a duration to set the range of the timeline. Options are **1 hour**, **3 hours**, and **5 hours**. The default is **1 hour**.
- **Timeline Slider**: The timeline slider determines the time window of all data displayed. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. For more customization of the timeline range, click and drag the boundary lines.

  Note The timeline can display data from up to two weeks in the past.

Step 6 Click **Run Packet Capture**.

The **Client Packet Capture** slide-in pane is displayed, and the **Onboarding Packet Capture** tab is selected by default.

Step 7 In the **Client Packet Capture** slide-in pane, click the **OTA Sniffer** tab.

The floor map view is displayed by default.

Step 8 Choose which APs to run radio or AP sniffing on by doing one the of the following:

- On the floor map, click the APs.
- Click the list icon in the view switcher, and then check the check boxes next to the APs.

  Catalyst Center displays only the radios that the OTA Sniffer supports.

Note The OTA Sniffer captures Wi-Fi packets on a specific AP radio's band and channel. The same AP radio can't be reused for OTA if it was previously used for OTA in the last 15 minutes. To re-enable OTA on the same AP radio, you must wait until the **Device 360** window for that AP radio displays new client-serving data.

Step 9 Click **Next**.

Step 10 Choose a band, radio, channel width, and channel from the respective drop-down lists.

Note For APs that support dual-radios, run the OTA sniffer data packet capture using either the primary or secondary radio, as follows:

- When dual-radio mode is disabled on the AP, use the primary radio to do the data packet capture.
- When dual-radio mode is enabled on the AP, use the secondary radio to do the data packet capture.

Step 11 Click **Next**.

Step 12 If a **Warning** dialog box about changing radio modes and losing client connectivity displays, click **OK** to acknowledge and continue.

Step 13 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 14 In the **Task Name** field, modify the task name if necessary.

Step 15 Click **Apply**.

Step 16 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

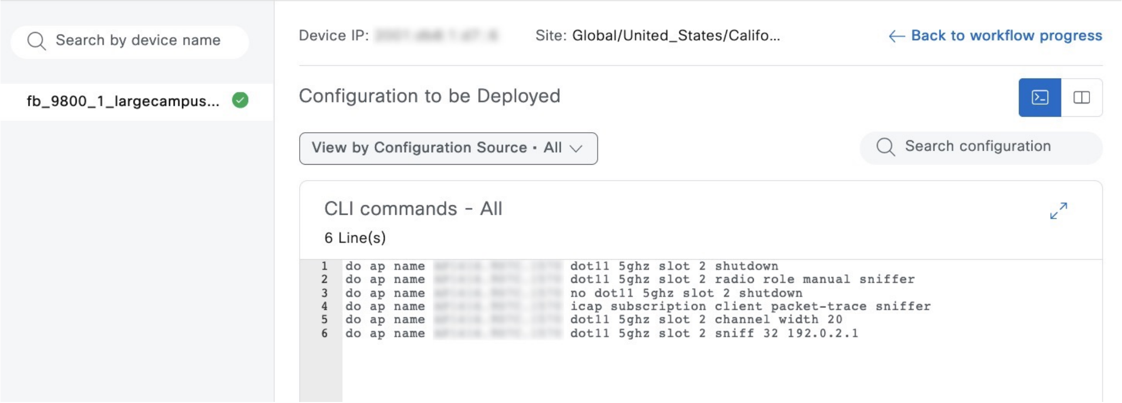
Step 17 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Note When reviewing the device configurations under **Configuration to be Deployed**, the configured destination IP address is ignored at the device level. For example, in the following figure, you can see the destination IP address is configured as 192.0.2.1. Instead of sending the packet data to the destination IP address, it is sent to Catalyst Center.



Device IP: [redacted] Site: Global/United_States/Califo...

Configuration to be Deployed

CLI commands - All

6 Line(s)

```
do ap name [redacted] dot11 5ghz slot 2 shutdown
do ap name [redacted] dot11 5ghz slot 2 radio role manual sniffer
do ap name [redacted] no dot11 5ghz slot 2 shutdown
do ap name [redacted] icap subscription client packet-trace sniffer
do ap name [redacted] dot11 5ghz slot 2 channel width 20
do ap name [redacted] dot11 5ghz slot 2 sniff 32 192.0.2.1
```

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

Note

- All OTA Sniffer Capture sessions are displayed under **Assurance** > **Intelligent Capture Settings** > **OTA Sniffer**. OTA Sniffer data captures are divided into separate 500-MB files. There is a 15-GB limit on the total size of all OTA Sniffer Capture files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 15-GB limit. Additionally, any OTA sniffer capture files that are more than 24 hours old are removed, even if the total size limit has not been reached.
- Because the OTA Sniffer Capture duration is 15 minutes, Catalyst Center automatically runs enable and disable tasks. To view the configuration preview of the enable or disable tasks, go to the **Tasks** window, open the task, and click **View Work Item Details**. If you don't view the configuration preview before the task completes, the option to preview will no longer be available.

Download PCAP Files from a Completed OTA Sniffer Capture Session

You can download the PCAP files from a completed OTA Sniffer Capture session from one of the following windows:

- **Device 360**: When you download the PCAP files from the **Device 360** window, only the data from the completed OTA Sniffer Capture sessions for that specific device are downloaded.
- **Client 360**: When you download the PCAP files from the **Client 360** window, the data from both the completed Full Packet Capture and OTA Sniffer Capture sessions for that specific client are downloaded.
- **Intelligent Capture Settings**: Under the **OTA Sniffer Capture** > **Completed Captures** tabs on the **Intelligent Capture Settings** window, only the data of selected APs from the completed OTA Sniffer Capture sessions are downloaded.

The following procedure shows you how to download the PCAP files from the **Intelligent Capture Settings** window.

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

Step 2 On the **Intelligent Capture Settings** window, click the **OTA Sniffer Capture** tab.

On the **OTA Sniffer Capture** window, the **In-progress Captures** tab is selected by default.

Step 3 Click the **Completed Captures** tab.

The **Completed Captures** table lists the completed OTA Sniffer Captures sessions.

Step 4 Under the **Download** column, click the down arrow icon corresponding to the relevant completed capture session to download its PCAP files.

The data packet files contain information on wireless data, which includes 802.11 files for packets moving between the AP and the client.

Note Data packet captures are divided into separate 100-MB files. There is a 4-GB limit on the total size of all data packet capture files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 4-GB limit. Additionally, any data packet capture files that are more than 14 days old are removed, even if the total size limit has not been reached.

AP Statistics Capture for APs and Wireless Controllers

About AP Statistics Capture for APs and Wireless Controllers

The Intelligent Capture feature allows you to enable or disable AP Statistics Capture on specific APs and capable wireless controllers. When it's enabled, the following data is captured:

- AP radio and WLAN statistics, which are displayed in the **RF Statistics** tab of the **Device 360** > **Intelligent Capture** window.
- AP Client statistics (30-second samples), which are displayed in the **RF Statistics** area of the **Client 360** > **Intelligent Capture** window for all clients associated with the selected APs.

Enable or Disable AP Statistics Capture on a Specific AP

You can enable and manage one or more APs to capture AP Statistics data, including AP radio statistics, WLAN statistics, and AP Client statistics. Catalyst Center can support up to 1000 APs for AP Statistics Capture.

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

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Under **Configure AP Enablement**, click **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Step 4 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected, and a list of disabled APs on the selected floor is displayed.

Note If you want to enable or disable AP Statisitics Capture on all APs managed by a wireless controller and the **Global - enable or disable capable WLCs** radio button is dimmed, you must first disable this feature on all enabled APs listed under the **Enabled APs** tab.

Step 5 Do one of the following:

- To enable AP Statistics Capture on specific APs, proceed to Step 6, on page 20.
- To disable AP Statistics Capture on specific APs, click the **Enabled APs** tab and proceed to Step 6, on page 20.

Step 6 Check the check boxes next to the APs that you want to enable or disable AP Statistics Capture on.

Step 7 Do one of the following:

- To enable AP Statistics Capture on the selected APs, click **Enable**.
- To disable AP Statistics Capture on the selected APs, click **Disable**.

Step 8 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 9 In the **Task Name** field, modify the name if necessary.

Step 10 Click **Apply**.

Step 11 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 12 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

Enable or Disable AP Statistics Capture on a Wireless Controller

You can enable or disable AP Statistics Capture on capable wireless controllers. You can enable up to three wireless controllers. When this feature is enabled, all APs managed by the wireless controller capture AP Statistics data, including AP radio statistics, WLAN statistics, and AP Client statistics.

Catalyst Center can support up to 1000 APs for AP Statistics Capture.

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

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Under **Configure AP Enablement**, click **Global - enable or disable capable WLCs** and then click **Get Started**.

Step 4 In the **Warning** dialog box, click **Yes** to continue.

Note If you want to enable or disable AP Statistics Capture on specific APs and the **Specific - select specific APs and enable** radio button is dimmed, you must first disable this feature on all enabled wireless controllers.

The **AP Stats Capture** tab is selected, and the table lists capable wireless controllers. Under the **Configuration Status** column, one of the following statuses is displayed for each wireless controller:

- **Success**: Catalyst Center successfully enabled AP Statistics Capture on the wireless controller.
- **Not Configured**: Catalyst Center has not enabled AP Statistics Capture on the wireless controller.
- **In Progress**: Catalyst Center is enabling AP Statistics Capture on the wireless controller.
- **Failed**: Catalyst Center failed to enabled AP Statistics Capture on the wireless controller because the wireless controller didn't accept the configuration.

  Tip If the **Configuration Status** is **Failed**, disable AP Statistics Capture on the wireless controller and then re-enable it on the wireless controller.

- **Unknown**: Catalyst Center enabled AP Statistics Capture on the wireless controller, but Catalyst Center doesn't know the device status.

  Tip If the **Configuration Status** is **Unknown**, disable AP Statistics Capture on the wireless controller and then re-enable it on the wireless controller.

Step 5 Check the check boxes next to the wireless controllers that you want to enable or disable AP Statistics Capture on.

Step 6 Do one of the following:

- To enable AP Statistics Capture on all APs managed by wireless controllers, click **Enable**.
- To disable AP Statistics Capture on all APs managed by wireless controllers, click **Disable**.

Step 7 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 8 In the **Task Name** field, modify the name if necessary.

Step 9 Click **Apply**.

Step 10 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 11 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item's approval status or the task's deployment status on the **Tasks** window. If the work item isn't approved, you need to resubmit the work item for ITSM approval. When it's approved, it's deployed at the scheduled time.

View Incompatible APs for AP Statistics Capture

You can view incompatible APs for AP Statistics Capture only when you choose **Specific - select specific APs and enable** for the type of AP enablement.

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

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Under **Configure AP Enablement**, click **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Step 4 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected, and a list of disabled APs on the selected floor is displayed.

Step 5 Click the **Not-Ready APs** tab.

Note Incompatible APs have the following conditions:

- The operation mode is not set to `local` or `FlexConnect`.
- The OS release that is installed on the AP is not compatible. The OS release must be MR1 or later.

View RF Statistics of an AP

You can view RF statistics of a specific AP using the following procedure.

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

The **Overall** health dashboard is displayed.

Step 2 Click the **Network Health** tab.

The **Network Health** window is displayed.

Step 3 Do one of the following:

- From the **Network Devices** dashlet, click the device name (hyperlinked identifier) for the AP to view the details for the AP.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the AP is displayed.

Step 4 In the **Device 360** window, click **Intelligent Capture** at the top-right corner.

The **Intelligent Capture:** *AP Name* window is displayed.

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** is displayed next to the AP name, see Client or Access Point Unable to Send Intelligent Capture Data to Catalyst Center, on page 37.

Step 5 Click the **RF Statistics** tab to view details about RF statistics.

Note If **AP Stats Capture** has not been enabled, enable it. See Enable or Disable AP Statistics Capture on a Specific AP, on page 20 or Enable or Disable AP Statistics Capture on a Wireless Controller, on page 22.

Step 6 Use the timeline to view the RF statistics for a given time and specify the scope of the data:

Timeline Slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and choose a duration to set the range of the timeline. Options are **1 hour** (the default), **3 hours**, and **5 hours**.
Timeline Slider	The timeline slider determines the time window of all data displayed. The timeline slider is color-coded to display the health of the AP. You can hover your cursor at a specific time to see details such as the device health score, system resources, and data plane. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. For more customization of the timeline range, click and drag the boundary lines.

Step 7 Use the radio frequency selector under the timeline to filter the data in the dashlets based on the frequency bands.

Click the drop-down list and choose **Radio 0 (2.4 GHz or 5 GHz)**, **Radio 1 (5 GHz)**, or **Radio 2 (6 GHz)** (depending on the number of radios supported).

Step 8 Use the dashlets to view the RF statistics details:

Note You can do the following in the charts that are displayed in the dashlets:

- Hover your cursor over the charts to view details.
- Click and drag within the chart to zoom in on a period. To change the view to the default, click 🔍.
- Click the color-coded data types below the chart to disable or enable the data type that is displayed in the chart.

Dashlets	Description
Clients dashlet	Displays the number of clients using the AP. The data source is from the AP WLAN statistics.

Dashlets	Description
Top Clients with Tx Failed Packets by SSID dashlet	Displays the list of SSIDs in the table. The data source for the table is from the AP WLAN statistics. The data source for the bar chart is from AP client statistics. Choose an SSID to see the top clients with transmit failed packets for that SSID.
Channel Utilization dashlet	Displays the channel utilization percentage used by the AP and other wireless and non-wireless devices. The data source for the bar chart is from AP Radio Statistics.
Channel Utilization by this Radio dashlet	Displays the current channel utilization percentage used by the AP and a list of SSIDs, the number of clients connected to it, and the number of packets sent or received over the last 15 minutes for its clients. The data source for the table is from the AP WLAN statistics. The data source for the circle chart is from AP radio statistics.
Frame Count dashlet	Displays the number of management and data frames. The data source is from the AP radio statistics.
Frame Errors dashlet	Displays the number of transmit and receive errors. The data source is from the AP radio statistics.
Tx Power and Noise Floor dashlet	Displays the transmit power and noise floor. The data source is from the AP radio statistics.
Multicast/Broadcast Counter dashlet	Displays the multicast and broadcast counts for each SSID. The data source is from the AP WLAN statistics.

Anomaly Capture for APs and Wireless Controllers

About Anomaly Capture for APs and Wireless Controllers

The Intelligent Capture feature allows you to enable or disable Anomaly Capture on a specific AP or wireless controller. When it's enabled, all anomaly onboarding events for all clients that are associated with the selected APs are captured for download or display.

AP Capture Limitation

There is a 1.05-GB limit on the total size of all anomaly triggered packet files that reside on Catalyst Center. If the limit is exceeded, packet files are removed, starting with the oldest, until the total size falls below the 1.05-GB limit.

Enable or Disable Anomaly Capture on a Specific AP

You can enable and manage one or more APs to capture anomaly onboarding events of all clients that are associated with one or more APs. Enabling Anomaly Capture ensures that all anomaly onboarding events for all clients associated with the selected APs are captured for download and display. Disabling Anomaly Capture ensures that all anomaly onboarding events for all clients associated with the selected APs are not captured for download and display.

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

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Click the **Anomaly Capture** tab.

Step 4 Under **Configure AP Enablement**, click the **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Note If you want to enable or disable Anomaly Capture on all APs managed by a wireless controller and the **Global - enable or disable capable WLCs** radio button is dimmed, you must first disable this feature on all enabled APs listed under the **Enabled APs** tab.

Step 5 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected, and a list of disabled APs on the selected floor is displayed.

Note If a previous attempt to enable the AP failed, an error message is displayed in the **Config Status** column.

Step 6 Do one of the following:

- To enable Anomaly Capture on specific APs, proceed to Step 7, on page 27.
- To disable Anomaly Capture on specific APs, click the **Enabled APs** tab and then proceed to Step 7, on page 27.

Step 7 Check the check boxes next to the APs that you want to enable or disable Anomaly Capture on.

Step 8 Do one of the following:

- To enable Anomaly Capture on the selected APs, click **Enable**.
- To disable Anomaly Capture on the selected APs, click **Disable**.

Step 9 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 10 In the **Task Name** field, modify the name if necessary.

Step 11 Click **Apply**.

Step 12 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.

- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 13 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item’s approval status or the task’s deployment status on the **Tasks** window. If the work item isn’t approved, you need to resubmit the work item for ITSM approval. When it’s approved, it's deployed at the scheduled time.

Enable or Disable Anomaly Capture on a Wireless Controller

You can enable or disable Anomaly Capture on capable wireless controllers, and you can enable up to three wireless controllers. Enabling Anomaly Capture ensures that all anomaly events of clients associated with APs managed by the wireless controller are captured for download and display. Disabling Anomaly Capture ensures that all anomaly onboarding events of clients associated with APs managed by the wireless controller are not captured for download and display.

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

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Click the **Anomaly Capture** tab.

Step 4 Under **Configure AP Enablement**, click **Global - enable or disable capable WLCs** and then click **Get Started**.

Step 5 In the **Warning** dialog box, click **Yes** to continue.

Note If you want to enable or disable Anomaly Capture on specific APs and the **Specific - select specific APs and enable** radio button is dimmed, you must first disable this feature on all enabled wireless controllers.

The **Anomaly Capture** tab is selected, and the table lists capable wireless controllers. Under the **Configuration Status** column, one of the following statuses is displayed for each wireless controller:

- **Success**: Catalyst Center successfully enabled Anomaly Capture on the wireless controller.
- **Not Configured**: Catalyst Center has not enabled Anomaly Capture on the wireless controller.
- **In Progress**: Catalyst Center is enabling Anomaly Capture on the wireless controller.
- **Failed**: Catalyst Center failed to enabled Anomaly Capture on the wireless controller because the wireless controller didn't accept the configuration.

  Tip If the **Configuration Status** is **Failed**, disable Anomaly Capture on the wireless controller and then re-enable it on the wireless controller.

- **Unknown**: Catalyst Center enabled Anomaly Capture on the wireless controller, but Catalyst Center doesn't know the device status.

  Tip If the **Configuration Status** is **Unknown**, disable Anomaly Capture on the wireless controller and then re-enable it on the wireless controller.

Step 6 Check the check boxes next to the wireless controllers that you want to enable or disable Anomaly Capture on.

Step 7 Do one of the following:

- To enable Anomaly Capture on all APs managed by the selected wireless controllers, click **Enable**.

  If the **Warning** dialog box (about not being able to make any further changes until the AP enablement is complete) displays, click **Yes** to continue.

- To disable Anomaly Capture on all APs managed by the selected wireless controllers, click **Disable**.

Step 8 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 9 In the **Task Name** field, modify the name if necessary.

Step 10 Click **Apply**.

Step 11 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 12 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item’s approval status or the task’s deployment status on the **Tasks** window. If the work item isn’t approved, you need to resubmit the work item for ITSM approval. When it’s approved, it's deployed at the scheduled time.

View Incompatible and Supported APs for Anomaly Capture

You can view incompatible and supported APs for Anomaly Capture only when you choose **Specific - select specific APs and enable** for the type of AP enablement.

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

Step 2 On the **Intelligent Capture Settings** window, click the **Access Point** tab.

On the **Access Point** window, the **AP Stats Capture** tab is selected by default.

Step 3 Click the **Anomaly Capture** tab.

Step 4 Under **Configure AP Enablement**, click the **Specific - select specific APs and enable** and then click **Get Started**.

The left pane displays the left tree hierarchy, and the right pane displays the default view because no floor is selected.

Step 5 In the left pane, expand **Global** and drill down to the site > building > floor.

In the right pane, the **Disabled APs** tab is selected and a list of disabled APs on the selected floor is displayed.

Step 6 To view incompatible APs for Anomaly Capture, click the **Not-Ready APs** tab.

Note Incompatible APs have the following conditions:

- The operation mode is not set to `local` or `FlexConnect`.
- The OS release that is installed on the AP is not compatible. The OS release must be MR1 or later.

Step 7 To display the list of APs that support Intelligent Capture, click the information icon next to the **Not-Ready APs** tab.

Spectrum Analysis for APs

About Cisco AP Functionality During Spectrum Analysis

The Cisco Aironet 2800 Series, 3800 Series, and 4800 Series Access Points (APs) have dual band radios with flexible radio assignment (FRA) in slot 0. This FRA radio operates on 2.4 GHz, but can be assigned to operate on 5 GHz. Its mode can be changed to differ from the AP's operational mode. When you configure the AP's FRA radio to operate in 5 GHz, no client radios can operate in 2.4 GHz band.

Note Spectrum Analysis is *not supported* on the Aironet 1540 AP, Aironet 1800 Series APs, and Catalyst 9115 AP.

Note Verify that the APs have the correct software version installed. See the **Supported Cisco APs** table in the Supported Devices for Intelligent Capture, on page 1 topic.

Radio slot assignments for spectrum analysis are as follows:

Device Model	Spectrum Analysis Radio Slot Assignment
Aironet 2800 Series APs Aironet 3800 Series APs Aironet 1560 APs Catalyst IW6300 Heavy Duty Series APs Catalyst IW6300 Heavy Duty Series APs	Radio slots 0 and 1 are enabled.
Aironet 4800 Series APs Catalyst 9120 AP Catalyst 9130 APs	These APs have three radio slots. If data packet capture is running, radio slots 0 and 1 are enabled. If data packet capture is not running, radio slot 2 is enabled. **Note** AP spectrum analysis data is not displayed for the 2.4 GHz channel band. Also, if there is no AP radio serving the 2.4 GHz band, the **Radio Mode** and **Channel** fields are empty. This occurs if the FRA radio is set to operate in 5 GHz and packet capture is enabled.

Start a Spectrum Analysis Session on an AP

You can start a spectrum analysis session on a specific AP using the following procedure.

Note

- The duration of a spectrum analysis session is 10 minutes.
- The maximum number of concurrent spectrum analysis sessions is 10.

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

Step 2 Click the **Network Health** tab.

Step 3 Do one of the following:

- From the **Network Devices** dashlet, click the device name (hyperlinked identifier) for the AP to view the details for the AP.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the AP is displayed.

Step 4 In the **Device 360** window, click **Intelligent Capture** at the top-right corner.

The **Intelligent Capture:** *AP Name* window is displayed.

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** is displayed next to the AP name, see Client or Access Point Unable to Send Intelligent Capture Data to Catalyst Center, on page 37.

Step 5 Click the **Spectrum Analysis** tab.

Step 6 Click **Start Spectrum Analysis**.

Step 7 In the slide-in pane, depending on the Visibility and Control of Configurations settings, choose an available option:

- **Now**: Immediately deploy the configurations.
- **Later**: Schedule the date and time and define the time zone of the deployment.
- **Generate configuration preview**: Review the configurations before deploying them.

  If only visibility is enabled or both visibility and control are enabled, **Generate configuration preview** is chosen by default, and **Now** and **Later** are dimmed (unavailable). For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

Step 8 In the **Task Name** field, modify the name if necessary.

Step 9 Click **Apply**.

Step 10 On the **Performing Initial Checks** window, address the following issues to continue with your current deployment:

- Pending Operations: Wait for all pending operations to deploy or discard them.
- Device Compliance: Fix, acknowledge, or ignore all issues.

  If you ignore any noncompliant devices, this activity is captured on the **Audit Logs** window.
- After addressing all the issues, click **Recheck** in the bottom-right corner of the window and make sure that all the validations are successful.

For more information, see "Network Provisioning Prechecks" in the *Cisco Catalyst Center User Guide*.

If you chose **Now** or **Later**, click **Submit**, and the device configurations will deploy at the scheduled time. You can view the task on the **Tasks** window.

Step 11 If you chose **Generate configuration preview**, depending on the Visibility and Control of Configurations settings, do the following:

a. On the **Preparing Devices and Configuration Models** window, wait for the system to prepare the devices and generate the device configurations. This can take some time, so you can click **Exit and Preview Later**. To view the work item later, go to the **Tasks** window.

b. On the **Preview Configuration** window, review the device configurations.

For more information, see "Visibility and Control of Wireless Device Configurations" in the *Cisco Catalyst Center User Guide*.

c. Do one of the following:

- When you're ready, click **Deploy** or **Submit for Approval**.
- If you're not ready to deploy the configurations or submit them for ITSM approval, click **Exit and Preview Later**. Later, go to the **Tasks** window, open the work item, and click **Deploy** or **Submit for Approval**.

Note You can submit the device configurations for ITSM approval and deploy them without previewing all the configurations.

d. In the slide-in pane, indicate when you want to deploy the configuration, choose a time zone, and if visibility and control are enabled, add notes for the IT administrator.

e. Click **Submit**.

You can check the work item’s approval status or the task’s deployment status on the **Tasks** window. If the work item isn’t approved, you need to resubmit the work item for ITSM approval. When it’s approved, it's deployed at the scheduled time.

Note Based on the 10-minute spectrum analysis duration, Catalyst Center automatically runs enable and disable tasks for the capture session. To view the configuration preview of the enable and disable tasks, go to the **Tasks** window, open the task, and click **View Work Item Details**. If you don't view the configuration preview before the task completes, the option to preview is no longer available when it completes.

View Spectrum Analysis Data of an AP

You can view the spectrum analysis data of an AP using the following procedure.

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

Step 2 Click the **Network Health** tab.

Step 3 Do one of the following:

- From the **Network Devices** dashlet, click the device name (hyperlinked identifier) for the AP to view the details for the AP.
- In the **Search** field (located at the top-right corner), enter the device name, IP address, or MAC address.

A 360° view of the AP is displayed.

Step 4 In the **Device 360** window, click **Intelligent Capture** at the top-right corner.

The **Intelligent Capture:** *AP Name* window is displayed.

Attention If a ⚠ icon with the message **GRPC link is not ready (CONNECTING)** is displayed next to the AP name, see Client or Access Point Unable to Send Intelligent Capture Data to Catalyst Center, on page 37.

Step 5 Click the **Spectrum Analysis** tab.

Step 6 Use the timeline to view the spectrum analysis data for a given time and specify the scope of the data to display:

Timeline Slider	
Item	**Description**
1 hour drop-down list	Click the drop-down list and choose a duration to set the range of the timeline. Options are **1 hour** (the default), **3 hours**, and **5 hours**.

Timeline Slider	
Item	**Description**
Timeline Slider	The timeline slider determines the time window of data that is displayed. The timeline slider is color-coded to display the health of the AP. You can hover your cursor at a specific time to see the details, such as the device health score, system resources, and data plane. For Spectrum Analysis, the time range is set to a 5-minute window. To adjust the timeline to a different time window, click the < and > buttons to the desired time window. **Note** The timeline can display data from up to two weeks in the past. Click and drag the boundary lines to view data for a specific time.

Step 7 Use the radio frequency selector under the timeline to filter the data in the charts based on the frequency bands. Click **2.4 GHz**, **5 GHz**, or **6 GHz**.

Note If **Radio Mode** and **Channel** (above the **Spectrum Analysis** charts) do not display any data, this indicates that the AP has no radios operating on the selected band. This occurs when an AP has both the client serving radios operating on **5 GHz**, while the radio frequency selector is set to **2.4 GHz**.

For more details, see About Cisco AP Functionality During Spectrum Analysis, on page 31.

Step 8 Use the **Spectrum Analysis** charts for the following functionality:

Spectrum Analysis Charts	
Item	**Description**
Top chart (Persistence)	This chart provides in real time the amplitude (power) and the channel frequency for each heard signal in the RF environment. The X axis represents the amplitude and the Y axis represents the channel frequency. The colors in the chart represent how many signals are heard at the same amplitude and channel frequency within the selected 5-minute time period: • Blue indicates a low number of overlapping signals (or signals heard at the same amplitude and frequency). • Red indicates a high number of overlapping signals. The intensity of the color increases (from blue > green > yellow > orange > red) as more signals are heard. As the lines in the chart overlap and intersect, they change color. The transparency of the colors represents the age of the signal data, with older data being more transparent. To view the RF environment in real time, click **Realtime FFT** (Fast Fourier Transform) to enable it. Enabling Realtime FFT limits the persistence chart to display "one" most recent data stream, rather than a collection of data streams from a 5-minute time period. To zoom in and view data for a specific range of channels, click and drag your mouse to choose the range. The chart refreshes and displays data for the specific channels that you selected. To zoom out and view the entire chart, click the magnifying glass on the top-right corner.
Bottom chart (Waterfall)	This chart provides a time-wise interpretation of data. The chart provides the same information as the Persistence chart but in a different format. The X axis shows the time and the Y axis shows the channel frequency. The lines in the chart represent the exact order in which the events have occurred, which can enable you to troubleshoot the root cause if a problem occurs. The colors in the chart represent the amplitude. Blue indicates a low value (-100 dBm) and red indicates a high value (-20 dBm).

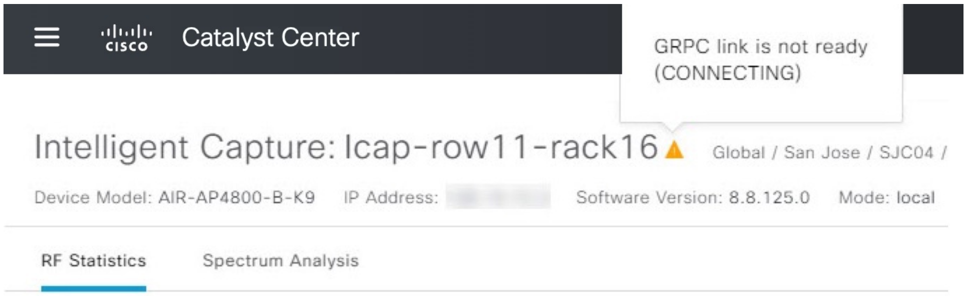
Step 9 Use the **Interference and Duty Cycle** chart to view the following:

- Detected interference and its severity:
  - Interference is plotted as a circle where the radius represents the bandwidth of the interference. The X axis represents the frequency in which the interference was heard on and the Y axis represent the severity.
  - Severity measures the impact of the interference and the range. Range is from 0, which indicates no impact, to 100, which indicates a huge impact.
  - The interference type is determined by its RF signature, which is identified by Cisco CleanAir Technology.
- The duty cycle of each channel.

Troubleshoot Intelligent Capture

Client or Access Point Unable to Send Intelligent Capture Data to Catalyst Center

Problem: Client or access point is unable to send Intelligent Capture data to Catalyst Center. The warning (⚠) icon appears with the message **GRPC link is not ready (CONNECTING)**:



Catalyst Center

GRPC link is not ready (CONNECTING)

Intelligent Capture: Icap-row11-rack16 ⚠ Global / San Jose / SJC04 /

Device Model: AIR-AP4800-B-K9 IP Address: [redacted] Software Version: 8.8.125.0 Mode: local

Background: In order for APs to send Intelligent Capture data to Catalyst Center, the Intelligent Capture port number on the Cisco Catalyst 9800 Series Wireless Controller or Cisco Wireless Controller must be set to 32626. Typically, when the Catalyst 9800 Series Wireless Controller or wireless controller is discovered by Catalyst Center, the port number is automatically set to 32626.

However, there are some upgrade paths for Catalyst Center that can cause the port number from being properly set.

Solution: To resolve this issue, do the following:

1. Check that the Catalyst 9800 Series Wireless Controller or wireless controller has the Intelligent Capture server port number is set to 32626.
2. If the port number is not set to 32626, manually set it.