Monitor the Rogue and aWIPS Dashboard

Access the Rogue Management and aWIPS Application

Step 1 To access the Rogue Management and aWIPS application, log in to Cisco DNA Center.

Step 2 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS**.

The **Rogue and aWIPS** dashboard is displayed.

Note Before using the Cisco DNA Assurance application, you must configure it. For more information, see Basic Setup Workflow.

Monitor the Rogue Management and aWIPS Dashboard

Use the Rogue and aWIPS dashboard to get a detailed threat analysis and a global view of all the rogue APs and aWIPS signatures detected in the network. The Rogue and aWIPS dashboard also provides insight into the highest-priority threats so that you can quickly identify them. The Rogue Management application uses streaming telemetry to retrieve data on rogue APs.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS**.

The **Rogue and aWIPS** window is displayed. By default, Cisco DNA Center displays the **Overview** tab.

Note If a Cisco AireOS Controller does not meet the minimum software version, a notification appears at the top of the dashboard. Click **Go To Devices** in the notification to upgrade to the supported version.

Step 2 From the **Actions** drop-down list, you can perform the following functions:

Choose **Rogue** > **Enable** to enable rogue detection on the Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controller.

The rogue management functionality is enabled by default if it is already enabled while migrating from Cisco DNA Center Release 1.3.3.x to Cisco DNA Center Release 2.2.1.0 or later.

Step 3 Choose **Rogue** > **Disable** to disable the rogue actions temporarily.

Step 4 Click **Yes** in the **Warning** dialog box that appears.

After disabling the rogue management functionality, data from the wireless controller will not be pushed to Cisco DNA Center until the rogue management functionality is enabled.

Step 5 Choose **Status** to view the rogue configuration job status.

Step 6 Filter the rogue configuration status by **All**, **Failure**, **Success**, or **In Progress** by clicking the respective tabs.

The **Operation** column shows **Enable** if the rogue-detection operation is enabled successfully on the wireless controller.

The **Status** column shows **Success** if the configuration changes are successfully pushed to the wireless controller.

Step 7 Choose **aWIPS** > **Enable** to enable aWIPS data collection on Cisco DNA Center.

If you are migrating from Cisco DNA Center Release 1.3.3.x to Cisco DNA Center Release 2.2.1.0 or later, you must enable the aWIPS functionality in Cisco DNA Center Release 2.2.1.0 or later.

Step 8 Choose **aWIPS** > **Disable** to disable aWIPS actions temporarily.

Step 9 Click **Yes** in the **Warning** dialog box that appears.

Step 10 Choose **aWIPS** > **Status** to view the aWIPS subscription status.

Step 11 Filter the aWIPS configuration status by **All**, **Failure**, **Success**, or **In Progress** by clicking the respective tabs.

The **Operation** column shows **Enable** if the aWIPS detection operation is enabled successfully on the wireless controller.

The **Status** column shows **Success** if the configuration changes are successfully pushed to the wireless controller.

Step 12 Move the timeline slider to view data about a threat that occurred at a specific time.

The **Active High Threats** and **High Threats Over Time** graphs below the timeline slider display the threat details accordingly.

Step 13 Click the **Show Map** icon to get a global map view of sites in your network.

- The **Active High Threats** and **High Threats Over Time** graphs display information about rogue APs detected in the last 3 hours by default. The graph information is based on the time interval that you choose from the hours drop-down list.

  The options are **Last 3 hours**, **Last 24 hours**, and **Last 7 days**.

- The **Active High Threats** widget presents information about threat levels in the form of a donut graph. Hover your cursor over the graph to see the number of rogue APs found in each threat level.

- The **High Threats Over Time** graph presents information about high threats over, time based on the time interval that you choose from the time interval drop-down list. Hover your cursor over the graph to view the number of high threats that occurred at a particular time.

- The **Threats** table displays a list of rogue APs found on the network.

Step 14 Some columns are hidden in the default column view setting. To customize the columns, click the three dots at the right-end of the column heading.

Step 15 Click and choose a layout preset: **Basic** or **All**.

Step 16 Click the Filter icon at the left end of the **Threats** table to narrow down the rogue AP list based on the following criteria: **ID**, **Threat Level**, **Threat MAC Address**, **Type**, **State**, **Connection**, **Detecting AP**, **Detecting AP Site**, **RSSI (dBM)**, **SSID**, **Clients**, **Containment Status**, **Last Reported**, and **Vendor**.

RSSI, **SSID**, and **Clients** are not displayed for aWIPS.

The following information is displayed for each rogue AP found on the network:

- **ID**: Rogue AP identifier.
- **Threat Level**: Color-coded classified threat level. Cisco DNA Center classifies threats into these categories:
  - **High Threat**
  - **Potential Threat**
  - **Informational**
- **Threat Mac Address**: MAC address of the rogue AP.
- **Type**: Threat types for rogue AP and aWIPS.

  The available classification types for Rogue AP are:
  - **Beacon DS Attack**
  - **AP Impersonation**
  - **Allowed List**
  - **Rogue on wire**
  - **Honeypot**
  - **Interferer**
  - **Allowed Vendor**
  - **Friendly**
  - **Neighbor**
  - **Custom Rule Name**
- The available signature types for aWIPS are:
  - **EAPOL logoff flood**
  - **Deauthentication broadcast**
  - **CTS Flood**
  - **RTS Flood**
  - **Deauthentication flood**
  - **Disassociation broadcast**

- **Disassociation flood**
- **Broadcast probe**
- **Association flood**
- **Authentication flood**
- **Deauthenticatioon Flood**
- **Fuzzed Beacon**
- **Fuzzed Probe Request**
- **Fuzzed Probe Response**
- **PS Poll Flood**
- **EAPOL Start V1 Flood**
- **Reassociation Request Flood**
- **Beacon Flood**
- **Probe Response Flood**
- **Block Ack Flood**
- **Airdrop Session**
- **Malformed Association Request**
- **Authentication Failure Flood**
- **Invalid MAC OUI Frame**
- **Malformed Authentication**
- **CTS Virtual Carrier Sense Attack**
- **RTS Virtual Carrier Sense Attack**

- **State**: Shows the state of the rogue AP/aWIPS attacks.
- **Source/Target**: Shows whether the displayed MAC address is the source of an aWIPS attack or target of an aWIPS attack. This column is not applicable for rogue data.
- **Connection**: Whether the rogue AP is located on the wired network or wireless network. This column shows the aWIPS attacks always on the wireless network.
- **Detecting AP**: Name of the AP that is currently detecting the rogue AP. If multiple APs detect the rogue, the detecting AP with the highest signal strength is displayed. This column is applicable for rogue AP and aWIPS attacks.
- **Detecting AP Site**: Site location of the detecting AP. This column is applicable for rogue AP and aWIPS attacks.
- **RSSI (dBm)**: RSSI value reported by the detecting AP. RSSI (dBm) is only applicable for rogue AP.
- **SSID**: Service Set Identifier that the rogue AP is broadcasting. SSID is only applicable for rogue AP.
- **Clients**: Number of rogue clients associated to this access point. This column is only applicable for rogue AP.

- **Wireless Containment Status**: Show the possible values (Contained, Pending, Open, & Partial) of a rogue AP. Wireless containment status is only applicable for rogue AP.
- **Last Reported**: Date, month, year, and time when the rogue AP/aWIPS attack was last reported.
- **Vendor**: Rogue AP vendor information. This column is not applicable for aWIPS attacks.

Obtain Rogue AP Details from the Threat 360° View

You can quickly view the location details of a specific rogue AP on a floor map within the **Threat 360°** view.

You can get precise location details for a specific rogue AP on the floor map depending on the detecting AP's strongest signal strength, or x and y coordinate information from Cisco Connected Mobile Experiences (CMX), when x and y coordinates are available.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS**.

Step 2 To launch the **Threat 360°** view for a particular AP, click the corresponding rogue AP row in the **Threats** table.

The **Threat 360°** pane appears.

The upper part of the pane displays the following information:

- MAC address of the rogue AP
- Threat level
- Threat type
- Status
- Vendor
- Containment
- Count
- Last reported

The middle part of the pane shows the estimated location of a rogue AP or a threat on the floor map:

- Site details and floor number.
- Floor map shows the names of the managed APs.

Step 3 Perform the following tasks, as required:

- Click the  icon at the right-hand corner of the floor map to see the IP address of the wireless controller that manages APs along with the reachability status.
- Click the  icon at the right-hand corner of the floor map to zoom in on a location. The zoom levels depend on the resolution of an image. A high-resolution image provides more zoom levels. Each zoom level comprises a

different style map that is shown at different scales, each one showing the corresponding details. Some maps are of the same style, but at a smaller or larger scale.

- Click the icon to see a map with fewer details.
- Click the icon to view the map icon legend.

The following table provides descriptions of the floor map icons.

Table 1: Map Icons and Descriptions

Floor Map Icon	Description
Devices	
	Access Point
	Sensor
	Rogue AP
	Marker
Average Health Score	
	Health score: 8-10
	Health score: 4-7
	Health score:1-3
	Health score: Unknown
AP Status	
	Covered by sensor
	Not covered by sensor

Step 4 The bottom area of the pane enables you to perform these tasks:

- Click the **Switch Port Detail** tab to get details about rogue on wire, including information such as **Host Mac**, **Device Name**, **Device IP**, **Interface Name**, **Last Updated**, **Port Mode**, and **Admin Status**.

Note
- **Admin Status** column shows interface status either as **UP** or as **DOWN**.
- **Port Mode** column shows the interface mode either as **ACCESS** or as **TRUNK**.

Note Cisco switches are required for rogue-on-wire detections.

- Click the **Detections** tab to view information such as **Detecting AP**, **Detecting AP Site**, **Adhoc**, **Rogue SSID**, **RSSI (dBM)**, **Channels**, **Radio Type**, **SNR**, **State**, and **Last Updated**.
- Click the **Filter** ( ) icon at the left end of the table to narrow down the search results based on **Rogue SSID**, **RSSI**, **Radio Type**, **Security**, and **SNR**.
- Click the **Export** icon and save it to your system.
- Click the **Clients** tab to view details such as **MAC Address**, **Gateway Mac**, **Rogue AP Mac**, **IP Address**, and **Last Heard**about the clients that are associated with the rogue AP.
- Click the **Filter** ( ) icon at the left end of the table to narrow down the results based on your search criteria.

Download aWIPS Profile Forensic Capture from the Threat 360° View

This procedure describes how to download the forensic capture of various denial of service (DoS) attacks from the Threat 360 view.

Note Cisco DNA Center enables or disables forensic capture only on default-ap profile. You must enable or disable forensic capture in case of brownfield deployments where you have created Custom AP Join Profiles.

Before you begin

You must verify the network connectivity between the access points and Cisco DNA Center.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon ( ) and choose **Workflows** > **Rogue and aWIPS**.

Step 2 In the **Rogue and aWIPS** dashboard, scroll down to view the **Threat** table.

Step 3 In the **Threat MAC address** column, click the aWIPS attack link.

Threat 360 window appears.

Step 4 Click **Forensic Capture** tab to view the information such as **Detecting AP**, **Alarm ID**, **CaptureFilename**, and **Last Updated**.

Step 5 In the **Capture Filename** column, click the **pcap** file to download the aWIPS profile forensic capture.

Step 6 Click **Download All** to download all the **pcap** files.

Step 7 Click the **Filter** icon to narrow down the search results based on **Detecting AP**.

Step 8 Click the **Export** icon to save the **CSV** file it to your workspace.

Note Cisco DNA Center shows a maximum of 50 forensic captures at a time.