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   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   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** dashboard.

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

Step 2   In **Site** menu, click **Global**.

The **Site Selector** slide-in pane is displayed.

a) You can enter a site name in the **Search Hierarchy** search bar or expand **Global** to choose a site.

Note   • If the site has more than 254 sub sites, the site will be disabled by default.

• Site hierarchies that do not have floors inside them are not listed in the site selector.

Step 3   From the **Actions** drop-down list, choose **Rogue** > **Enable** to enable rogue detection on the Cisco Wireless Controller and the 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 4   Choose **Rogue** > **Disable** to disable the rogue actions temporarily.

Step 5   Click **Yes** in the **Warning** dialog box that is displayed.

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 6   Choose **Rogue** > **Status** to view the rogue configuration job status.

Step 7   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 8   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 9   Choose **aWIPS** > **Disable** to disable aWIPS actions temporarily.

Click **Yes** in the **Warning** dialog box that is displayed.

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   Use the Threats dashlets for the following information:

• **TOTAL ROGUE THREATS**: Displays total number of rogue threats.

• **TOTAL AWIPS THREATS**: Displays total number of AWIPS threats.

• **TOTAL UNIQUE ROGUE CLIENTS**: Displays total number of unique rogue clients.

• **ROGUES CONTAINED**: Displays total number of rogue contained.

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

Step 13 The **Active High Threats**, **Top Locations Affected** 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**.

     Note   Choose **Custom** to select specific time range.

Step 14 Use **High Threats Summary** dashlet for following information:

High Threats Summary Dashlet	
Item	**Description**
Active High Threats	Displays information about active threat levels in the form of a donut graph. You can filter the active high threats by threat types, **Top 10** or **All**.
	Click on each colored slice of donut graph, that displays detailed information of the threats in the threats table. Hover your cursor over the graph to see the number of active high threats.
	Click **All** to display threat type and count in a table form.
Top Locations Affected	Displays top 5 locations affected per selected site for high threats.

Step 15 Use **High Threats Over Time** dashlet for following information:

High Threats Over Time Dashlet	
Item	**Description**
Threats Over Time	Displays detailed information about high threats over time, based on the selected time period.
	Click on each threat type available below **Total Active High Threat**, it displays threat information in graph view.
	High threat deviation is measured on a scale of value to value:
	• Green colour indicates threat deviation less than 0.
	• Orange colour indicates threat deviation from 0 to 9.
	• Red colour indicates threat deviation more than or equal to 10.
	Hover your cursor over the graph to view the number of high threats that occurred at a particular time.
View Threats	Click **View Threats** to view threats table, it displays list of high threats.

Step 16 Use **Threats By Location** dashlet to view information about threats in map view.

Location Option	
Item	**Description**
Map View	Click this toggle button to display locations affected by threats in the map view. Hover your cursor over desired location in map to view all the threat level and counts.
List View	Click this toggle button to display information about locations affected by threats in a list view.

Step 17 Use **Threat Setting Summary** dashlet to view following information:

Threat Setting Summary Dashlet	
Item	**Description**
Allowed AP List	Displays information about allowed AP count and configured threat level. Click **View Details** to display **Allowed List** window, for detailed information on **Allowed Access Point List**.
Allowed Vendor List	Displays information about total allowed vendors count and configured threat level. Click **View Details** to display **Allowed List** window, for detailed information on **Allowed Vendor List**.
Rogue Rule	Displays information about rules, its conditions type, rule profiles associated to it and threat level. Click **View Details** to display **Rules** window, for detailed information on **Rogue Rules.**

Step 18 (Optional) Use **Tips** dashlet, that provides direct link to use the workflows such as Create Allowed AP List, Create Allowed Vendor List, Create Rogue Rule, and so on.

Click **View All** to view all the available workflows.

Monitor Rogue Threats Of Your Network.

Step 1 In **Site** menu, click **Global**.

The **Site Selector** slide-in pane is displayed.

a) You can enter a site name in the **Search Hierarchy** search bar or expand **Global** to choose a site.

Note	• If the site has more than 254 sub sites, the site will be disabled by default.
	• Site hierarchies that do not have floors inside them are not listed in the site selector.

the window:

Step 2   Click the time range setting (🕐) at the top-right corner to specify the time range of the data that you want displayed on the threats table.

    a) From the drop-down menu, choose a time range: **3 hours**, **24 hours**, **7 days** or **Custom**.

    b) For **Custom** time range, specify the **Start Date** and time; and the **End Date** and time.

    c) Click **Apply**.

Step 3   Use the **Threat Table** to view detailed information about threats in your network.

Threats Table	
Item	**Description**
▼ **Filter Icon**	Click this icon at the top-right corner of the **Threats** table to filter the data to be displayed in the table 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.

Monitor Rogue Threats Of Your Network.

Threats Table	
Item	**Description**
Threat Table	

Threats Table

Item	Description
	Displays the following information about threats in a table format. Threats table displays the following information:

- **Threat Level**: Displays Color-coded classified threat level. Cisco DNA Center classifies threats into these categories:

  - **High Threat**

  - **Potential Threat**

  - **Informational**

- **Mac Address**: Displays MAC address of the rogue AP.

- **Type**: Displays threat types.

- **State**: Displays State of the rogue AP or aWIPS attacks.

- **Source/Target**: Displays whether the displayed MAC address is the source of an aWIPS attack orthe target of an aWIPS attack. This column is not applicable for rogue data.

- **Connection**: Displays whether the rogue AP is located on the wired network or wireless network. This column shows the aWIPS attacks on the wireless network.

- **Detecting AP**: Displays name of the AP that is currently detecting a rogue AP. If multiple APs detect a rogue, the detecting AP with the highest signal strength is displayed. This column is applicable for rogue AP and aWIPS attacks.

- **Detecting AP Site**: Displays site location of the detecting AP. This column is applicable for rogue AP and aWIPS attacks.

- **RSSI (dBm)**: Displays RSSI value reported by the detecting AP. RSSI (dBm) is only applicable for rogue AP.

- **SSID**: Displays service set identifier that the rogue AP is broadcasting. SSID is only applicable for rogue AP.

- **Clients**: Displays number of rogue clients associated with this AP. This column is only applicable for rogue AP.

Note	The client count that is displayed in the **Threats** table differs from the client count displayed in the **Threats 360 degrees** window. This happens if the data that is processed in a release of Cisco DNA Center earlier than release 2.3.2 is migrated to Cisco DNA Center 2.3.2 or later. Cisco DNA Center 2.3.2 or later displays the correct client count for the newly processed data if the time range that is selected has the new data.

- **Containment Status**: Displays the possible values (**Contained**, **Pending**, **Open**, and **Partial**) of a rogue AP. Wireless containment status is only applicable for rogue APs.

- **Last Reported**: Displays date, month, year, and time when a rogue AP or aWIPS attack was last reported.

- **Vendor**: Displays rogue AP vendor information. This column is not applicable for aWIPS

Threats Table	
Item	**Description**
	attacks.
⚙	Customize the data that you want displayed in the table: a. From the **Table Appearance** tab, set the table density and striping. b. From the **Edit Table Columns** tab, check the check boxes for the data that you want displayed in the table. c. Click **Apply**.

Obtain Rogue AP and Rogue Client Details from the Threat 360° View

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

You can get precise location details for a specific rogue AP or rogue client on the floor map depending on the detecting AP's strongest signal strength. With the Cisco Connected Mobile Experiences (CMX) or Cisco DNA Spaces integration, you can get the exact location of your rogue AP or rogue client.

Step 1   Click the menu icon (≡) and choose **Assurance** > **Rogue and aWIPS** > **Threats**.

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

The **Threat 360°** pane is displayed.

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 the 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 a map icons 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
	Planned AP
	Switch
	Interferer
	Client
	Rogue Client

Floor Map Icon	Description
	Reporting AP
	Detecting AP
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
  - The **Admin Status** column shows interface status as either **UP** or **DOWN**.

  - The **Port Mode** column shows the interface mode as either **ACCESS** or **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 DoS attacks from the Threat 360 view.

Note Cisco DNA Center enables or disables forensic capture only on the default AP profile. You must enable or disable forensic capture in case of existing 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 Click the menu icon (≡) and choose **Workflows** > **Rogue and aWIPS** > **Threats**.

Step 2 In the **Threat MAC address** column, click the aWIPS attack link.

The **Threat 360** window is displayed.

Step 3 Click the **Forensic Capture** tab to view information such as **Detecting AP**, **Alarm ID**, **CaptureFilename**, and **Last Updated**.

Step 4 In the **Capture Filename** column, click the **pcap** file to download the aWIPS profile forensic capture.

Step 5 Click **Download All** to download all the **pcap** files.

Step 6 Click the **Filter** icon to narrow down the search results based on **Detecting AP**.

Step 7 Click the **Export** icon to save the **CSV** file to your workspace.

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