



Monitor Rogue and aWIPS Dashboard

- [Access the Rogue Management and aWIPS Application, on page 1](#)
- [Monitor the Rogue Management and aWIPS Dashboard, on page 1](#)
- [Obtain Rogue AP Details from the Threat 360° View, on page 4](#)
- [aWIPS Profiles, on page 6](#)
- [Download aWIPS Profile Forensic Capture from the Threat 360° View, on page 10](#)

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.

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, you must enable the aWIPS functionality in Cisco DNA Center Release 2.2.1.0.

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**
- 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**
- **State:** Shows the state of the rogue AP/aWIPS attacks.
 - **Source/Target:** Shows the threat MAC address that is source and target of 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	



Floor Map Icon	Description
	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**, **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.

aWIPS Profiles

The Cisco DNA Center aWIPS profile allows you to configure thresholds used in detection of aWIPS denial of service (DoS) attacks and enables/disables a particular aWIPS DoS attack.

The aWIPS profile configuration support is available only for the following network devices with software version 17.4:

- Cisco Catalyst 9800 Series Wireless Controller for cloud
- Cisco Catalyst 9800 Series Wireless Controller
- Cisco Embedded Wireless Controller on Catalyst Access Points (EWC-APs)
- Cisco Embedded Wireless Controller installed on Cisco Catalyst 9300 Series Switches
- Cisco Catalyst 9400 Series Switches
- Cisco Catalyst 9500 Series Switches



Note On 9300, 9400, and 9500 wireless series switches, wireless module must be enabled for aWIPS profiles to work.

Before you begin

- Ensure that the network device downloads the aWIPS profile configuration from Cisco DNA Center. The network device must be reachable from Cisco DNA Center.
- For aWIPS profile configuration, you must verify the network connectivity between the wireless controller and Cisco DNA Center.
- For forensic capture, you must verify the network connectivity between the access points and Cisco DNA Center.
- For forensic capture to work, a gRPC tunnel must be established between the access point and Cisco DNA Center. To do this, use **show ap icap connection** command and make sure the status is READY.
- For forensic capture, the required ports must be opened between Cisco DNA Center and network device link.
- For forensic capture, there should not be a time lag between Cisco DNA Center and access point.

Step 1

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance > Rogue and aWIPS > aWIPS Profile**. The **aWIPS Profile** dashboard appears.

Note When you navigate to the **aWIPS Profile** tab for the first time, an error message appears on the top of the **aWIPS Profile** dashboard to subscribe the upgraded subscription even if the **aWIPS** is enabled in the Cisco DNA Center. To subscribe the upgraded subscription, you must disable and enable the **aWIPS** from the **Rogue and aWIPS** overview dashboard, see [Monitor the Rogue Management and aWIPS Dashboard](#).

The aWIPS Profile dashboard displays the following information:

- **Profile Name:** Shows the list of aWIPS profiles names.
- **Assigned WLCs:** Shows the number of assigned wireless controllers to an aWIPS profile.
- **Last Changed:** Shows the last created or updated date and time of an aWIPS profile.

Step 2 Click **Add Profile** to add an aWIPS profile.

Note You cannot create more than 100 aWIPS profiles.

Step 3 In the **Profile Name** column, click the aWIPS profile name to edit an aWIPS profile.

Step 4 To assign an aWIPS profile at device level, check the check box next to the aWIPS profile name and choose **More Actions > Assign**.

Note You cannot assign more than one aWIPS profile to the device at a time.

Step 5 To delete an aWIPS profile, check the check box next to the aWIPS profile name and choose **More Actions > Delete**.

Step 6 In the **Assigned WLCs** column, click the number link to view the number of wireless controllers assigned to an aWIPS profile.

The **Profile Assigned to WLC** window shows the following attributes of the network device:

- **Device Name:** Shows the name of the network device.
- **IP Address:** Shows the IP address of the network device.
- **Profile Config URL Push Status:** Shows the status of profile configuration URL push to the network device. The possible values of push status are **Success**, **Failure**, and **In Progress**.

In case of **Failure** status, hover your mouse over the **i** icon next to the **Failure** to see the failure reason.

- **Profile Config Download Status (On Device):** Shows the profile configuration download status on the device. The possible values of download status are **Success**, **Failure**, and **In Progress**.

In case of **Failure** status, hover your mouse over the **i** icon next to the **Failure** to see the failure reason.

Note

- If aWIPS subscription is disabled on Cisco DNA Center, an error message appears on the top of the **aWIPS Profile** dashboard. You must have aWIPS subscription to see the value of **Profile Config Download Status (On Device)**. To subscribe the aWIPS data collection, enable the **aWIPS** from the **Rogue and aWIPS** overview dashboard, see [Monitor the Rogue Management and aWIPS Dashboard](#).

- The HTTP protocol reachability must be present between the device and Cisco DNA Center for device to download the Profile configuration from profile config URL.

- **Forensic capture config Status:** Shows the forensic capture config status on **default-ap-profile** AP Join Profile on the device. The possible values of config status are **Success**, **Failure**, and **In Progress**.

In case of **Failure** status, hover your mouse over the **i** icon next to the **Failure** to see the failure reason.

- **Forensic Capture:** Shows whether the forensic capture is enabled/disabled on **default-ap-join** AP Join Profile on the device. Forensic capture on custom AP join profile is not yet supported.

Hover your mouse over the **i** icon next to the Forensic capture, a tooltip saying **Shows the current Forensic Capture status on default-ap-profile AP Join Profile on the device** appears.

Note

- In the **Profile Assigned to WLC** window, you cannot enable or disable the **Forensic Capture**.

- **Assigned On:** Shows the date and time of aWIPS profile assigned to wireless controller.

Edit an aWIPS Profile

This procedure describes how to edit an aWIPS profile.

Before you begin

To subscribe the additional subscription, you must disable and enable the **aWIPS** from the **Rogue and aWIPS** overview dashboard, see [Monitor the Rogue Management and aWIPS Dashboard](#).

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance > Rogue and aWIPS > aWIPS Profile**. The **aWIPS Profile** dashboard appears.
- Step 2** In the **Profile Name** column, click the aWIPS profile link that you want to edit. The **Edit aWIPs Profile** window appears.
- Note** You cannot edit a default aWIPS profile.
- Step 3** In the **Signature** column, check the check box next to the aWIPS signature that you want to select or deselect for the chosen aWIPS profile.
- Step 4** In the **Configure Threshold** column, for the chosen aWIPS signature, enter the threshold value within the specified range that is displayed on the top of respective **Configure Threshold** name field.
- Note** The **Configure Threshold** value cannot be in alphanumeric format.
- Step 5** In the **Forensic Capture** column, click the toggle button to enable or disable the forensic capture for the chosen aWIPS signature.
- Note** The Cisco DNA Center does not allow you to make any changes in the **Default Threshold** value and **Time Interval (In Seconds)** value for aWIPS profile.
- Step 6** (Optional) Click **Reset to Default** to bring back the default aWIPS profile configuration.
- Step 7** Click **Save** to save the changes.
- The profile is saved and pushed to all the devices that are assigned to the given aWIPS profile.
- Note** In the Configure Threshold column, for the chosen aWIPS signature, if you enter the threshold value out of specified range an error message appears on the top of the **Edit aWIPs Profile** window to enter the correct value within the specified range.
-

Delete an aWIPS Profile

This procedure describes how to delete an aWIPS profile from Cisco DNA Center.

Before you begin

To subscribe the additional subscription, you must disable and enable the **aWIPS** from the **Rogue and aWIPS** overview dashboard, see [Monitor the Rogue Management and aWIPS Dashboard](#).

-
- Step 1** In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance > Rogue and aWIPS > aWIPS Profile**. The **aWIPS Profile** dashboard appears.
- Step 2** In the **aWIPS Profile(s)** table, check the check box next to the aWIPS profile name that you want to delete.
- Note**
- You cannot delete a default aWIPS profile.
 - You cannot delete an aWIPS profile which is assigned to the network device. Instead, you must reassign the device to the default aWIPS profile and then delete it.
- Step 3** From the **More Actions** drop-down list, choose **Delete**.
- Step 4** In the subsequent warning window, click **Delete**.
-

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.

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.
-