Cisco DNA Center Rogue Management and aWIPS Application Quick Start Guide, Release 2.2.3

First Published: 2021-08-04

Last Modified: 2023-06-26

CONTENTS

CHAPTER 1

Cisco DNA Center Rogue Management and aWIPS Application

Introduction to Rogue Management and aWIPS Application

Note In earlier versions of Cisco DNA Center, Rogue Management capabilities were provisioned as a part of Device Controllability. After a Cisco DNA Center upgrade, the provisioned Rogue Management subscriptions are not automatically removed from previously discovered Cisco Wireless Controllers. Rogue Management detection might be reported inconsistently on newly discovered wireless controllers.

The Rogue Management application is an optional package that you can install on Cisco Digital Network Architecture (DNA) Center. Operating within Cisco DNA Center, the Rogue Management application helps you monitor threats from unauthorized access points (APs). You can access the Rogue Management functionality as a dashboard within Cisco DNA Assurance in the Cisco DNA Center GUI.

Because the Cisco Adaptive Wireless Intrusion Prevention System (aWIPS) is integrated with Cisco DNA Center, you can monitor the aWIPS signatures within the Rogue and aWIPS dashboard.

This guide describes how to activate the Rogue and aWIPS application package on Cisco DNA Center. This guide also explains prerequisites and configurations, describes how to monitor the Rogue and aWIPS dashboard, and offers important notes and limitations.

The Rogue Management application supports the following Cisco AireOS Controller models running Cisco AireOS Release 8.8.111.0 or later.

- Cisco 3504 Wireless Controller

- Cisco 5520 Wireless Controller

- Cisco 8540 Wireless Controller

- Cisco Mobility Express

The following Cisco Catalyst 9800 Series Wireless Controller models support the Rogue Management application:

- Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches

- Cisco Catalyst 9800-40 Wireless Controller

- Cisco Catalyst 9800-80 Wireless Controller

- Cisco Catalyst 9800-CL Cloud Wireless Controller

- Cisco Catalyst 9800-L Wireless Controller

- Cisco Embedded Wireless Controller on Catalyst Access Points

The aWIPS supports Cisco Catalyst 9800 Series Wireless Controller Release 17.1.x, 17.2.x, and 17.3.x Cisco Catalyst 9100 Series Access Points, and Cisco 802.11ac Wave 2 Aironet Access Points.

The following Cisco Catalyst 9800 Series Wireless Controller models support the aWIPS application:

- Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches

- Cisco Catalyst 9800-40 Wireless Controller

- Cisco Catalyst 9800-80 Wireless Controller

- Cisco Catalyst 9800-CL Cloud Wireless Controller

- Cisco Catalyst 9800-L Wireless Controller

- Cisco Embedded Wireless Controller on Catalyst Access Points

About Rogue Management

The Rogue Management application in Cisco DNA Center detects and classifies threats and enables network administrators, network operators, and security operators to monitor network threats. Cisco DNA Center helps in quickly identifying the highest-priority threats and allows you to monitor these threats in the **Rogue and aWIPS** dashboard within Cisco DNA Assurance.

A rogue device is an unknown AP or client that is detected by the managed APs in your network. A rogue AP can disrupt wireless LAN operations by hijacking legitimate clients. A hacker can use a rogue AP to capture sensitive information, such as usernames and passwords. The hacker can then transmit a series of clear-to-send (CTS) frames. This action mimics an AP informing a particular client to transmit, while instructing all the others to wait. This results in legitimate clients not being able to access network resources. Therefore, wireless LAN service providers have a strong interest in banning rogue APs from air space.

Because rogue APs are inexpensive and readily available, employees sometimes plug unauthorized rogue APs into the existing LANs and build ad hoc wireless networks without the knowledge or consent of the IT department. These rogue APs can be a serious breach of network security when they are plugged into a network port behind the corporate firewall. Because employees generally do not enable any security settings on a rogue AP, it is easy for unauthorized users to use the AP to intercept network traffic and hijack client sessions. Even more alarming is that wireless users frequently publish insecure AP locations, which increases the odds of having enterprise security breaches.

Cisco DNA Center constantly monitors all the nearby APs and automatically discovers and collects information about rogue APs.

When Cisco DNA Center receives a rogue event from a managed AP, it responds as follows:

- If the unknown AP is not managed by Cisco DNA Center, Cisco DNA Center applies the rogue classification rules.

- If the unknown AP is not using the same SSID as your network, Cisco DNA Center verifies whether the AP is connected to the corporate wired network and extends to the wired network. If the rogue AP is physically connected to the switch port of the corporate network, Cisco DNA Center classifies the AP as **Rogue on wire**.

  Cisco switches managed by Cisco DNA Center are required for rogue on wire to work.

  Note There is a scenario in which an AP that is not rogue on wire may incorrectly get classified as rogue on wire by Cisco DNA Center. This incorrect classification happens when a rogue client roams from a rogue-on-wire AP to a nonrogue-on-wire AP. A new rogue client report with the new rogue AP information is received and a host entry for the client is available on Cisco DNA Center before the deletion of the rogue client information. This happens because it takes some time for the rogue client switch port details to get deleted on the switch and synchronized with Cisco DNA Center. Therefore, the new rogue AP that the client roamed to is classified as rogue on wire before the synchronization happens.

- If the AP is unknown to Cisco DNA Center, and is using the same SSID as your network, Cisco DNA Center classifies the AP as **Honeypot**.

  Note
  - The detected SSID that was earlier classified as Honeypot is not retained in the backup. Therefore, after a restore operation, the SSID is not classified as Honeypot.

  - Even if the SSID is deleted from the wireless controller, the SSID is still classified as Honeypot on Cisco DNA Center. The Honeypot classification does not happen when the detected SSID is not restored back on Cisco DNA Center when the Cisco DNA Center backup is restored.

- If the unknown AP is not using the same SSID as your network and is not connected to the corporate network, Cisco DNA Center verifies whether it is causing any interference. If it is, Cisco DNA Center classifies the AP as **Interferer** and marks the rogue state as **Potential Threat**. The threshold level for classifying the interferers on the network is greater than -75 dBm.

- If the unknown AP is not using the same SSID as your network, and is not connected to the corporate network, Cisco DNA Center verifies whether it is a neighbor. If it is a neighbor, Cisco DNA Center classifies the AP as **Neighbor** and marks the rogue state as **Informational**. The threshold level for classifying the rogue AP as a neighbor AP is less than or equal to -75 dBm.

About Advanced Wireless Intrusion Prevention System

The Cisco Advanced Wireless Intrusion Prevention System (aWIPS) is a wireless intrusion threat detection and mitigation mechanism. aWIPS uses an advanced approach to wireless threat detection and performance management. An AP detects threats and generates alarms. It combines network traffic analysis, network device and topology information, signature-based techniques, and anomaly detection to deliver highly accurate and complete wireless threat prevention.

With a fully infrastructure-integrated solution, you can continually monitor wireless traffic on both wired and wireless networks and use that network intelligence to analyze attacks from many sources to pinpoint accurately, and proactively prevent attacks, rather than wait until damage or exposure has occurred.

As the aWIPS functionality is integrated into Cisco DNA Center, the aWIPS can configure and monitor WIPS policies and alarms and report threats.

aWIPS supports the following capabilities:

- Static signatures

- Standalone signature detection

- Alarms

- Static signature file packaged with controller and AP image

Cisco DNA Center supports the following signatures that detect various denial of service (DoS) attacks:

- **Authentication flood**: A form of denial of service (DoS) attack that floods an APs client-state table (association table) by imitating many client stations (MAC address spoofing), and sending authentication requests to the AP. Upon reception of each individual authentication request, the target AP creates a client entry in State 1 of the association table. If open system authentication is used for the AP, the AP returns an authentication success frame and moves the client to State 2. If Shared Key Authentication (SHA) is used for the AP, the AP sends an authentication challenge to the attacker's imitated client, which does not respond, and the AP keeps the client in State 1. In either of these scenarios, the AP contains multiple clients hanging in either State 1 or State 2, which fills up the AP association table. When the table reaches its limit, legitimate clients are not able to authenticate and associate with this AP.

- **Association flood**: A form of DoS attack that aims to exhaust an AP's resources, particularly the client association table, by flooding the AP with many spoofed client associations. An attacker using such a vulnerability can emulate many clients to flood a target AP's client association table by creating many clients. When the client association table overflows, legitimate clients cannot get associated.

- **CTS Flood**: A form of DoS attack when a specific device sends a bulk CTS control packet to wireless devices sharing same RF medium and it blocks wireless devices from using RF medium until CTS flood stops.

- **RTS Flood**: A form of DoS attack when a specific device sends a bulk RTS control packet to AP for blocking wireless bandwidth that leads to performance disturbance for clients on that AP.

- **Broadcast Probe**: A form of DoS attack when a specific device tries to flood a managed AP with broadcast probe requests.

- **Disassociation Flood**: A form of DoS attack that aims to send an AP to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the AP to a client. With client adapter implementations, this form of attack is effective and immediate for disrupting wireless services against this client. Typically,

client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep the client out of service.

- **Disassociation Broadcast**: A form of DoS attack when a specific device triggers disassociation broadcast to disconnect all clients.

  This attack aims to send an AP's client to the unassociated or unauthenticated State 2 by spoofing disassociation frames from the AP to the broadcast address of all the clients. With current client adapter implementations, this form of attack immediately disrupts wireless services against multiple clients. Typically, client stations reassociate to regain service until the attacker sends another disassociation frame. An attacker repeatedly spoofs the disassociation frames to keep all the clients out of service.

- **Deauthentication flood**: A form of DoS attack that aims to send an AP's client to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the AP to the client unicast address. With the current client-adapter implementations, this form of attack immediately disrupts wireless services against the client. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame. An attacker repeatedly spoofs the deauthentication frames to keep all the clients out of service.

- **Deauthentication broadcast**: A form of DoS attack that sends all the clients of an AP to the unassociated or unauthenticated State 1 by spoofing deauthentication frames from the AP to the broadcast address. With client adapter implementation, this form of attack immediately disrupts wireless services against multiple clients. Typically, client stations reassociate and reauthenticate to regain service until the attacker sends another deauthentication frame.

- **EAPOL logoff flood**: A form of DoS attack when a specific device tries to send Extensible Authentication Protocol over LAN (EAPOL) logoff packets, which are used in the WPA and WPA2 authentication for (DoS).

  Because the EAPOL logoff frame is not authenticated, an attacker can potentially spoof this frame and log out a user from an AP, thus committing a DoS attack. The fact that the client is logged out from the AP is not obvious until the client attempts communication through the WLAN. Typically, the disruption is discovered and the client reassociates and authenticates automatically to regain the wireless connection. The attacker can continuously transmit the spoofed EAPOL-logoff frames.

- **Airdrop Session**: Airdrop session attack happens when an AirDrop, which is an Apple feature is used to set up a peer-to-peer link for file sharing. This potentially creates a security risk due to the unauthorized peer-to-peer network being dynamically created in your WLAN environment.

- **Authentication Failure Flood**: Authentication failure flood attack happens when a specific device tries to flood the AP with invalid authentication requests spoofed from a valid client leading to the disconnection.

- **Beacon Flood**: A form of DoS attack that allows an attacker to inhibit wireless activity for the entire enterprise infrastructure by preventing new associations between valid APs and stations. During a beacon flood attack, stations that are actively seeking a network are bombarded with beacons from networks-generated using different MAC addresses and SSIDs. This flood can prevent a valid client from detecting the beacons sent by the corporate APs, and hence a denial of service attack is initiated.

- **Block Ack Flood**: A form of DoS attack that allows an attacker to prevent an 802.11n AP from receiving frames from a specific valid corporate client. With the introduction of the 802.11n standard, a transaction mechanism was introduced which allows a client to transmit a large block of frames at once, rather than dividing them up into segments. In order to initiate this exchange, the client sends an Add Block Acknowledgment (ADDBA) to the AP, which contains sequence numbers to inform the AP of the size of the block being transmitted. The AP then accepts all frames that fall within the specified sequence

(consequently dropping any frames that fall outside of the range) and transmits a BlockACK message back to the client when the transaction has been completed.

- **EAPOL-Start V1 Flood**: EAPOL start flood is when an attacker attempts to bring down an AP by flooding it with EAPOL-Start frames to exhaust the internal resources of an AP.

- **Fuzzed Beacon**: Fuzzed Beacon is when an invalid, unexpected, or random data is introduced in the beacon and then replaying those modified frames into the air. This can cause unexpected behavior to the destination device including driver crashes, operating system crashes and stack based overflows which would allow execution of arbitrary code on the affected system.

- **Fuzzed Probe Request**: Fuzzed probe request is when an invalid, unexpected, or random data is introduced in the probe request and then replaying those modified frames into the air.

- **Fuzzed Probe Response**: Fuzzed probe response is when an invalid, unexpected, or random data is introduced in the probe response and then replaying those modified frames into the air.

- **Invalid MAC OUI Frame**: Invalid MAC OUI is when a spoofed MAC address is used which does not have a valid OUI.

- **Malformed Association Request**: Malformed association request is when an attacker sends a malformed association request which can trigger bug in AP leading to Denial of Service.

- **Malformed Authentication**: Malformed authentication is when an attacker sends malformed authentication frames which can expose vulnerabilities in some drivers.

- **Probe Response Flood**: A form of DoS that allows the attacker to prevent a station from associating to a valid corporate AP. In a typical wireless transaction, when a station wishes to associate to an AP, it transmits a probe request from to obtain information about the AP's network. The station will then wait for the resulting probe response frame from the AP. An attacker can take advantage of this process by flooding the environment with invalid probe responses, thus preventing the station from receiving the response from the valid AP. As a result, the station is rendered unable to connect to the wireless network, and a denial of service attack is initiated.

- **PS Poll Flood**: PS-Poll flood is when a potential hacker spoofs the MAC address of the wireless client and sends out a flood of PS-Poll frames. The AP then sends out the buffered data frames to the wireless client, which leads to client missing the data frames since it could be in the power save mode.

- **Reassociation Request Flood**: A form of DoS attack that exhausts AP's resources, particularly the client association table by flooding AP with a large number of emulated and spoofed client reassociations. Once the client association table overflows, legitimate clients are not able to get associated causing a DoS attack.

- **Targeted Deauthentication**: There is visibility into both source and destination of attacks for enhanced context of the threat.

- **CTS Virtual Carrier Sense Attack**: A form of DoS attack when MAC address of an 802.11n AP is modified that allows large duration values for CTS frame types by preventing channel access to legitimate users.

- **RTS Virtual Carrier Sense Attack**: A form of DoS attack when MAC address of an 802.11n AP is modified that allows large duration values for RTS frame types by preventing channel access to legitimate users.

Scale Information

This table shows the number of rogue APs and rogue clients supported on different versions of Cisco DNA Center appliance.

Table 1: Number of Rogue APs and Rogue Clients Supported

Cisco DNA Center Appliance	No. of Rogue APs Supported	No. of Rogue Clients Supported	No. of aWIPS Events per Day
44-core Cisco DNA Center appliance	24,000	32,000	20,000
56-core Cisco DNA Center appliance	24,000	32,000	30,000
112-core Cisco DNA Center appliance	96,000	128,000	65,000

Basic Setup Workflow

Step 1   Install Cisco DNA Center.

For more information, see the Cisco Digital Network Architecture Center Installation Guide.

Step 2   Download and install the **Rogue and aWIPS** application package.

For more information, see Download and Install the Rogue and aWIPS Application Package on Cisco DNA Center, on page 11.

Step 3   Verify that the Rogue and aWIPS application is in **Deployed** state.

To verify, from the Cisco DNA Center home page, click the **Gear** icon ⚙, and then choose **System** > **Setting** > **Installed Apps**.

Step 4   From this release onwards, you must enable Rogue and aWIPS application in the **Assurance** > **Rogue and aWIPS** window.

This enables rogue detection on the Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controllers.

To access the Rogue and aWIPS application, log in to Cisco DNA Center. In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Assurance** > **Rogue and aWIPS**.

Step 5   Discover devices such as Cisco Wireless Controller and APs using the Discovery feature.

Discover Cisco Wireless Controllers using the management IP address instead of the service port IP address.

Step 6   Make sure that the discovered devices are listed in the **Device Inventory** window.

The devices should be reachable and in **Managed** state in the **Device Inventory** window.

Step 7 Design your network hierarchy by adding sites, buildings, and floors so that later you can easily identify where to apply design settings or configurations later.

You can either create a new network hierarchy, or, if you have an existing network hierarchy in Cisco Prime Infrastructure, import it into Cisco DNA Center.

Step 8 Add the location information of APs and position the APs on the floor map to get a coverage heatmap visualization.

Step 9 (Optional) If your network uses Cisco Identity Services Engine (ISE) for user authentication, you can configure Cisco DNA Assurance for Cisco Identity Services Engine integration. This enables you to see more information about wired clients, such as the username and operating system, in Cisco DNA Assurance.

Step 10 (Optional) Configure syslog, SNMP traps, and NetFlow Collector servers using Telemetry.

Step 11 Start using the Cisco DNA Assurance application.

Step 12 (Optional) Integrate and synchronize Cisco Connected Mobile Experiences (CMX) with Cisco DNA Center.

You can get the 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 CMX.

Note If you do not have Cisco CMX integrated with Cisco DNA Center, the rogue AP will be displayed in the sitemap around the detecting AP with the strongest RSSI.

Related Documentation

Document	Information
Cisco DNA Center Installation Guide	Installation and configuration of Cisco DNA Center, including postinstallation tasks.
Cisco DNA Center Administrator Guide	Configuration of user accounts, Role-Based Access Control (RBAC) scope, security certificates, authentication and password policies, and global discovery settings. Monitoring and managing Cisco DNA Center services. Backup and restore procedures.
Cisco DNA Center User Guide	Use of the Cisco DNA Center GUI and its applications.
Cisco DNA Assurance User Guide	Use of the Cisco DNA Assurance GUI.
Release Notes for Cisco DNA Center	Release information, including new features and open and resolved bugs.
Cisco DNA Center Platform User Guide	Reports for Rogue and aWIPS.
Cisco DNA Center Platform Release Notes	Enablement of Rogue and aWIPS package in Cisco DNA Center platform.

Note   The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Install Cisco DNA Center Rogue Management Application Package

Application Management

Cisco DNA Center provides many of its functions as individual applications, that are packaged separately from the Cisco DNA Center core infrastructure. You can install and run the applications that you want and uninstall those that you are not using, depending on your preferences.

In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **System** > **Software Updates**. The number and type of application packages shown in the **Software Updates** window vary depending on your Cisco DNA Center version and licensing level. All available application packages are shown, whether or not they are currently installed.

For a description of a package and whether it is required, hover your cursor that package's name in the **Updates** tab in the **Software Updates** window.

Download and Install the Rogue and aWIPS Application Package on Cisco DNA Center

Before you begin

The Rogue Management and aWIPS application is not installed on Cisco DNA Center by default. You must manually download and install the Rogue and aWIPS application package separately.

Rogue Management requires a Cisco DNA Essentials license and aWIPS requires a Cisco DNA Advantage license.

You can perform the application management procedure from the **Software Updates** window.

1. Install Cisco DNA Center. For information, see the Cisco DNA Center Installation Guide.

2. Review the software requirements described in the release notes. For more information, see Related Documentation, on page 8.

> **Note** Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **System** > **Software Updates**.

The **Software Updates** window consists of the following tabs:

- **Updates**: Shows the system and application updates. **System Update** shows the installed system version, available system updates, and the system updates that you have downloaded from Cisco cloud. **Application Update** shows the available applications that can be downloaded and installed from Cisco cloud, the size of the application, and the appropriate action (**Download**, **Install**, or **Update**). Hover your cursor over the package to view the available version and a basic description.

- **Installed Apps**: Shows the installed application packages.

> **Note** After you navigate to the **Software Updates** window, a connectivity check is performed and the status is displayed. If there is a connectivity issue, the **Software Updates** window does not show new updates.

Step 2 To download the **Rogue and aWIPS** application, click **Install** next to the application name in **Software Updates** > **Updates** > **Application Updates**.

To update the **Rogue and aWIPS** application, click **Update** next to the application name in **Software Updates** > **Updates** > **Application Updates**.

> **Note** Ensure that the application is updated by reviewing the version in the **Installed Apps** window.

Step 3 After installing the package, you must enable the Rogue Management application.

a) In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Assurance** > **Rogue and aWIPS** to enable the Rogue and aWIPS application.

b) From the **Rogue** drop-down list that is located at the top-right corner of the **Rogue Management** window, choose **Enable**.

This enables rogue detection on the Cisco Wireless Controller and Cisco Catalyst 9800 Series Wireless Controllers.

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, on page 7.

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 2: 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.

aWIPS Profiles

About aWIPS Profiles

The aWIPS profile configuration allows you to select required signatures, configure threshold values used in detection of a WIPS denial of service (DoS) attacks, and enable forensic capture at signature level. Threshold configuration helps to adjust the number of alarms which are generated for a specific duration for each aWIPS signature.

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

- Cisco Catalyst 9800 Series Wireless Controller

- Cisco Catalyst 9800-CL Cloud Wireless Controller

- Cisco Embedded Wireless Controller on Catalyst Access Points

- Cisco Catalyst 9800 Embedded Wireless Controller for Catalyst 9300 Series Switches

- Cisco Catalyst 9400 Series Switches

- Cisco Catalyst 9500 Series Switches

Note You must enable wireless module on Cisco Catalyst 9300 Series Switches, Cisco Catalyst 9400 Series Switches, and Cisco Catalyst 9500 Series Switches for aWIPS profiles to work.

Prerequisites

- Verify the network connectivity between the Cisco Wireless Controller and Cisco DNA Center.

• Make sure that the network device is reachable from Cisco DNA Center and has downloaded the aWIPS profile configuration from Cisco DNA Center.

• For forensic capture, make sure that there is network connectivity between APs and Cisco DNA Center.

• For forensic capture, make sure that the Google Protocol RPC (gRPC) tunnel interface has been established between APs and Cisco DNA Center. Use the **show ap icap connection** command to make sure that the status is READY.

• For forensic capture, the required ports must be opened between Cisco DNA Center and network device links.

• For forensic capture, there should not be a time lag between Cisco DNA Center and access points.

• If you have upgraded Cisco DNA Center from an earlier release, you must disable and enable **aWIPS** from the **Rogue and aWIPS** dashboard to subscribe an additional subscription. For more information, see Monitor the Rogue Management and aWIPS Dashboard.

Note For a new installation of Cisco DNA Center, you do not have to disable and enable **aWIPS** from the **Rogue and aWIPS** dashboard to subscribe an additional subscription.

Create an aWIPS Profile Configuration Workflow

This section provides information about how to create an aWIPS profile.

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

You can also create an aWIPS profile by navigating to **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** > **Add Profile**.

The **Create an aWIPS Profile** window appears.

Step 2 Click **Let's Do it**.

The **aWIPS Profile Creation** window appears.

Step 3 In the **Profile Name** field, enter a name for the aWIPS profile.

Step 4 The **Signatures** table lists the following aWIPS profile parameters:

• **Signature**: Shows the standard aWIPS signatures that detect the various denial of service (DoS) attacks.

• **Default Threshold**: Shows the predefined threshold value for the respective aWIPS signature.

• **Configure Threshold**: Shows the manually configured threshold value for the respective aWIPS signature.

• **Time Interval (In Seconds)**: Shows the time interval of packets.

• **Forensic Capture**: Captures the aWIPS DoS attack packets in real time for the given signature.

Step 5   In the **Signature** column, check the check box next to the aWIPS signature that you want to select or deselect for an aWIPS profile.

If an aWIPS signature is not selected for an aWIPS profile, Cisco DNA Center does not detect the DoS attack for that particular aWIPS signature.

Step 6   In the **Configure Threshold** column, for the chosen aWIPS signature, enter the threshold value within the specified range that is displayed on top of the respective **Configure Threshold** field.

For some signatures, the configuration threshold is not applicable. The threshold configuration value for those signatures is displayed as NA on top of the respective **Configure Threshold** field.

The **Configure Threshold** value cannot contain alphanumeric characters.

Step 7   In the **Forensic Capture** column, click the toggle button to enable or disable the forensic capture for a particular aWIPS signature.

> **Note**
> - Cisco DNA Center does not allow you to edit the **Default Threshold** value and **Time Interval (In Seconds)** value for the aWIPS profile.
> - If you enable forensic capture for an aWIPS signature, Cisco DNA Center allows you to download packets from the **Threat 360** window.
> - If you disable forensic capture for an aWIPS signature, Cisco DNA Center does not capture the aWIPS DoS attack for the given signature.
> - Enabling **Forensic Capture** for RTS Flood and CTS Flood signatures might impact the performance of Cisco DNA Center.

Step 8   (Optional) Click **Reset to Default** to get the default aWIPS profile configuration.

Step 9   Click **Next**.

> **Note**   In the **Configure Threshold** column, for the chosen aWIPS signature, if you enter the threshold value out of the specified range, an error message appears on top of the **Create an aWIPS Profile** window to enter the correct value within the specified range.

Step 10   In the **Profile Summary** window, the **Profile Summary** table displays the summary of the profile that was configured in the previous window.

Step 11   Click **Next**.

Step 12   In the **Profile Creation Done** page, click **Assign Profile to Device(s)** to assign this aWIPS profile to a device.

The **Assign aWIPS Profile** window appears.

You can also assign an aWIPS profile to a device on the **Assurance** > **Rogue and aWIPS** > **aWIPS Profile** page by checking the check box next to the aWIPS profile name and choosing **More Actions** > **Assign**.

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

Step 13   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 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 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 the aWIPS subscription is disabled on Cisco DNA Center, an error message appears on the top of the **aWIPS Profile** dashboard. You must have an aWIPS subscription to see the value of **Profile Config Download Status (On Device)**. To subscribe the aWIPS data collection, enable **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 the device to download the profile configuration from the profile config URL.

- **Forensic capture config Status**: Shows the forensic capture config status on the **default-ap-profile** AP Join Profile on the device. The possible values 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 the **default-ap-join** AP Join Profile on the device. Forensic capture on custom AP join profile is not 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 the aWIPS profile is assigned to the wireless controller.

Step 14   Click **Next**.

The **Profile Creation Done** window appears.

View aWIPS Profiles

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

The **aWIPS Profile(s)** dashboard appears.

Note	When you navigate to the **aWIPS Profile** tab for the first time, an error message appears on top of the **aWIPS Profile** dashboard to subscribe the upgraded subscription even if **aWIPS** is enabled in Cisco DNA Center. To subscribe the upgraded subscription, you must disable and enable **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.

Assign an aWIPS Profile to the Network Device

Before you begin

If you upgrade Cisco DNA Center from an earlier release, you must disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard to subscribe the additional subscription. See Monitor the Rogue Management and aWIPS Dashboard.

Note   For a new installation of Cisco DNA Center, you do not need to disable and enable **aWIPS** from the **Rogue and aWIPS** overview dashboard to subscribe the additional subscription.

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

The **Assign an aWIPS Profile** window appears.

To skip this screen in the future, check the **Don't show this to me again** check box.

Step 2   Click **Let's Do it**.

The **Assign aWIPS Profile** window appears.

Step 3   From the **Profile Name** drop-down list, choose the aWIPS profile name that you want to assign to a device.

Step 4   In the left pane, you can either search for a site by entering its name in the **Find Hierarchy** field, or expand **Global** to choose the sites.

You can also search for a network device by entering its name in the **Search Table** field.

The **Network Devices** table shows the **Device Name**, **IP Address**, **Software Version**, **Reachability**, and **Forensic Capture** of the device and lists the network devices in the following sections:

• **Reachable & Supported**: Shows the list of reachable and supported network devices with software version 17.4, and reachability status with a green check mark.

• **Not Reachable/Not Supported**: Shows the list of unreachable or unsupported network devices with software version 17.4. You cannot assign an aWIPS profile to unreachable or unsupported network devices.

Step 5   In the **Reachable & Supported** tab, check the check box next to the device that you want to assign to the selected aWIPS profile. You can either select all devices or an individual device.

You can assign an aWIPS profile to a maximum of 100 devices at a time.

Step 6 In the **Forensic Capture** column, click the toggle button to enable or disable the forensic capture for the chosen network device at the device level.

This configures forensic capture at the **default-ap-profile** AP join profile. Forensic capture configuration at the custom AP join profile is not supported.

Step 7 Click **Next**.

Step 8 In the **Profile and devices Mapped Summary** window, expand **aWIPS Profile Details** to view the configuration summary of the selected aWIPS profile, and **Device Map** to view the configuration summary of assigned devices.

Step 9 Click **Next**.

The **Profile Assignment to Devices initiated successfully** window appears.

Note The profile assignment to the devices takes some time to complete. You must wait before retrying the assignment process.

Step 10 To view the status of the assigned aWIPS profile to the device, click the **Go to Rogue and aWIPS Home Page** link. For more information, see View aWIPS Profiles.

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 **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**.

Step 2 In the **aWIPS Profile(s)** table, click the profile name that you want to edit.

Step 3 In the **Edit aWIPS Profile** window that appears, make the necessary changes and click **Save**.

You cannot edit the default aWIPS profile.

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 a threshold value that is out of the 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 **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 that 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 warning window, click **Delete**.

Rogue AP Containment on Wired and Wireless Network

Rogue AP Containment Overview

The Cisco DNA Center Rogue AP Containment feature contains the wired and wireless Rogue AP. In case of Wired Rogue AP Containment, Cisco DNA Center brings the **ACCESS** mode switchport interface to the **DOWN** state on which the rogue AP is attached. In case of **Wireless Rogue AP Containment**, Cisco DNA Center instructs the strongest detecting wireless controller to initiate the containment on wireless rogue BSSIDs. The wireless controller in turn instructs the strongest detecting AP for those BSSIDs to stream the deauthentication packets to disrupt the communication between the rogue AP and the wireless clients of the corresponding rogue AP.

Rogue AP containment is classified as:

- **Wired Rogue AP Containment**: The rogue AP MAC addresses classified as **Rogue on Wire** on the Cisco DNA Center rogue threat dashboard.

- **Wireless Rogue AP Containment**: The rogue AP MAC addresses classified as **Honeypot**, **Interferer**, or **Neighbor** on the Cisco DNA Center rogue threat dashboard.

Rogue AP Containment is supported on Cisco AireOS Controllers and Cisco Catalyst 9800 Series Wireless Controllers.

Note Containment is not supported on aWIPS threats.

Wired Rogue AP Containment

The Wired Rogue AP Containment feature allows Cisco DNA Center to shut down the ACCESS mode interface on the switch to which the Rogue AP is physically attached. Cisco DNA Center performs wired rogue AP containment only on ACCESS mode interfaces, because shutting down any other mode might bring the network down.

If the rogue AP is attached to non-ACCESS mode interfaces, the network admin must contain the interface either manually or through a CLI command.

This procedure describes how to perform wired rogue AP containment on an ACCESS mode interface classified as **Rogue on Wire** in Cisco DNA Center.

Before you begin

Download and install the Rogue and aWIPS application package. For more information, see Download and Install the Rogue and aWIPS Application Package on Cisco DNA Center.

Ensure that you have G write permission from the provision API, scheduler API, and rogue side to perform this procedure.

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

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

Step 3 Click the rogue AP MAC address in the **Threat MAC address** column, classified as **Rogue on Wire**.

The **Threat 360** window appears.

Step 4 Click the **Action** drop-down list and choose **Shutdown Switchport**.

A warning pop-up window shows the list of ACCESS mode interfaces to be shut down on the corresponding device.

Note The **Shutdown Switchport** option appears in the **Action** drop-down list only when the rogue AP MAC address is marked as **Rogue on Wire**. For more information, see the Cisco Rogue AP Containment Actions Compatibility Matrix, on page 33.

The **Shutdown Switchport** action is irreversible. You must manually bring the switchport back up.

Step 5 In the warning pop-up window, click **Yes**.

The **Threat 360** window shows the wired rogue AP containment status:

- A banner with a blue check mark indicates that the wired rogue AP containment request is in progress.

- A banner with a green check mark indicates that the wired rogue AP containment is initiated successfully on the corresponding interface.

- A banner with a red check mark indicates that the wired rogue AP containment request failed.

Note - After containment is initiated, it takes some time for the interface state to update from **Rogue on Wire** to another threat classification type.

- The **Rogue on Wire** classification type changes to another classification type upon the arrival of the next wireless rogue message for the same rogue AP.

If a rogue AP MAC address is classified as **Rogue on Wire**, but there are no ACCESS mode interfaces up to initiate the containment, Cisco DNA Center disables the **Shutdown Switchport** option in the **Action** drop-down list.

Note   You cannot initiate **Wireless Rogue AP Containment** unless the rogue AP to which it corresponds is as long as in the **Rogue on Wire** classification type. For more information, see Wireless Rogue AP Containment.

Wireless Rogue AP Containment

The Wireless Rogue AP Containment feature allows Cisco DNA Center to contain the wireless clients connected to a rogue AP.

Containment is illegal in some countries because it disrupts the communication between the clients attached to a rogue AP. Cisco DNA Center warns you about the legal consequences while initiating wireless rogue AP containment.

This procedure describes how to start and stop wireless rogue AP containment on wireless clients connected to a rogue AP**.**

Before you begin

Download and install the Rogue and aWIPS application package. For more information, see Download and Install the Rogue and aWIPS Application Package on Cisco DNA Center.

Ensure that you have write permission from the provision API and scheduler API to perform this procedure.

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

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

Step 3   To perform wireless rogue AP containment, click the rogue AP MAC address listed under the **Threat MAC address** column, marked as either **Honeypot**, **Interferer**, or **Neighbor** classification types.

Threat 360 window appears.

Note   A rogue AP MAC address comprises multiple rogue BSSIDs.

Step 4   Click the **Action** drop-down list and choose **Start Containment**.

A **Warning** pop-up window appears that shows the warning of legal consequences and a list of rogue BSSIDs to be contained on wireless controller.

Note   The **Start Containment** option appears in the **Action** drop-down list only when the rogues AP MAC address is marked as either **Honeypot**, **Interferer**, or **Neighbor** classification type. For more information, see the Cisco Rogue AP Containment Actions Compatibility Matrix.

Step 5   Click **Yes** in the warning pop-up window.

The **Threat 360** window shows the wired rogue AP containment status as follows:

   • Banner with a blue check mark indicates that the wireless rogue AP containment request is in progress.

   • Banner with a green check mark indicates that the wireless rogue AP containment request is submitted successfully to the strongest detecting AP. A red vertical line appears next to the strongest detecting AP based on the RSSI value.

- Banner with a red check mark indicates that the wireless rogue AP containment request has failed.

Note Once containment is initiated, it takes some time for the **Containment Status** column to update with another wireless containment status

In the **Threat 360** window, hover your curser over the **i** icon next to the **Containment** column. A tooltip saying **This always shows current Wireless Containment Status** appears.

Step 6 Cisco DNA Center allows you to monitor the **Containment Status** of a wireless rogue AP in the **Rogue and aWIPS** dashboard threat table within Cisco DNA Assurance.

Hover your curser over the **i** icon adjacent to **Containment Status** column to view the following possible values.

Table 3: Wireless Containment Status Possible Values

Wireless Containment Status	Meaning
Contained	Rogue AP actively contained by Wireless Controller
Pending	Wireless Controller has kept this Rogue in Containment Pending state
Open	Rogue AP is not contained
Partial	Some of the Rogue BSSID's are Open and rest of them are either in Contained/Containment Pending state.

Note For a rogue AP with the wireless containment status as **Partial**, an **i** icon appears adjacent to **Partial** state under the **Containment** column in the **Threat 360** window. Hover your curser over the **i** icon to view the current wireless containment status of **Rogue SSIDs**.

The wireless controller can keep the wireless rogue AP containment in pending state because of the following reasons:

- **Resource outage**: Once the rogue BSSID containment request is submitted, wireless controller puts the rogue BSSID containment either in **Containment** or **Containment Pending** state because of 3 rogue BSSIDs per radio limitation for client serving radios and 6 rogue BSSIDs per radio limitation for monitor mode. Once the radio exceeds specified limitation, next submitted rogue BSSID for containment goes to the pending state by the wireless controller until one of the rogue BSSIDs goes out of containment state.

- **Protected Management Frames (PMF)**: The wireless controller does not initiate the containment as long as the Protected Management Frames (PMF) is enabled on rogue BSSID and keeps the containment status in pending state. Once the PMF is disabled, wireless controller initiates the containment.

- **Dynamic Frequency Selection (DFS)**: The wireless controller keeps the containment status in pending state and does not attempt to contain the rogue BSSID if it broadcasts on the Dynamic Frequency Selection (DFS) channels. Once the rogue BSSID moves out of the DFS channel, wireless controller initiates the containment.

Step 7 To bring back all the rogue BSSIDs of wireless rogue AP marked as either **Contained**, **Pending** or **Partial** state to **Open** state, click the rogue AP MAC address listed under the **Threat MAC address** column.

The **Threat 360** window appears.

Step 8 Click the **Action** dropdown and choose **Stop Containment**.

Note   The **Stop Containment** option appears in the **Action** dropdown menu only when wireless rogue AP is either in **Contained**, **Pending** or **Partial** state. For more information, see the Cisco Rogue AP Containment Actions Compatibility Matrix.

- A blue check mark notification is displayed as a banner on the Threat 360 window, that shows the **Stop Containment** process is in progress on wireless rogue AP.

- A green check mark notification is displayed as a banner on the Threat 360 window, that shows the **Stop Containment** process is initiated successfully on wireless rogue AP.

Cisco Rogue AP Containment Actions Compatibility Matrix

This table shows the behavior of rogue AP containment actions for the current state of rogue APs on the **Threat 360** window.

Table 4: Rogue AP Containment Actions Compatibility Matrix

Rogue AP Threat Type	Wireless Rogue AP Current Containment State	Start Containment option in "Actions" Drop-Down List	Stop Containment option in "Actions" Drop-Down List
Beacon DS Attack	Open	Disabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled
AP Impersonation	Open	Disabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled
Rogue on Wire	Open/Contained/Pending/Partial	Not Visible **Shutdown Switchport** is shown	Not Visible **Shutdown Switchport** is shown
Allowed List	Open	Disabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled
Honeypot	Open	Enabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled
Interferer	Open	Enabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled
Friendly	Open	Disabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled

Neighbor	Open	Enabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled

View Tasks and Audit Logs of Rogue AP Containment

In case of containment failure, Cisco DNA Center allows you to view the tasks and audit logs of submitted requests of wired and wireless rogue AP containment.

Step 1 In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Activity**.

Step 2 In the **Activity** window, click the **Tasks** tab.

Step 3 In the **FILTERS** drop-down list, enter **ROGUE** in the **Search** field, or choose **ROGUE**.

A list of submitted requests of wired and wireless rogue AP containment appears.

Step 4 Click the containment request.

The **ROGUE** window appears, showing the rogue AP containment operation details, status, date, and time.

Step 5 Click the **Audit Logs** tab to view the rogue AP containment type and corresponding device IP address.

Note
- For Cisco AireOS, the containment request audit logs show the **CLI** commands.

- For Cisco Catalyst 9800 Series Wireless Controllers, the containment request audit logs show the **NETCONF** requests.

- For **Wired Rogue AP containment**, the audit logs show the CLI commands executed on the switch to bring the switchport down.

Custom Classification of Rogue APs

About Allowed List Workflow

The Cisco DNA Center Rogue Management and aWIPS workflow allows you to review and mark the MAC Address of rogue access points, that you want to move to the allowed list in a bulk, and process bulk allowed list of selected Access Point MAC addresses.

Rogue Management and aWIPS workflow supports APs that are associated with Cisco AireOS Controllers and Cisco Catalyst 9800 Series Wireless Controllers.

You can move the following rogue AP types to the allowed list using this workflow:

- Rogue on Wire

- Honeypot

- Interferer

- Neighbor

You cannot move the following rogue AP types to the allowed list using this workflow:

- Beacon DS Attack

- AP Impersonation

- Friendly

Set Up the Allowed List Workflow

This procedure shows how to move rogue AP MAC addresses to the allowed list in bulk. These addresses are ones that you do not want to report as high threat in Cisco DNA Center.

Before you begin

To perform the following task, you must have SUPER-ADMIN-ROLE or NETWORK-ADMIN-ROLE permissions.

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

The **Set up Rogue Management and aWIPS** window appears.

Step 2 Click **Let's Do it**.

To skip this screen in the future, check the **Don't show this to me again** check box.

The **Bulk upload allowed access points** window appears.

Step 3 In the **Search** field, you can search for the MAC addresses that were already added in the previous workflow.

Click **Export** to export the allowed list.

Step 4 You can download the sample CSV template file and manually add the MAC address, operation, and category to create the bulk allowed list template. Click the **Download the sample CSV template from here** link.

You can hover your cursor over the notification symbol to view the format of allowed MAC addresses, operations, and categories.

Step 5 You can either drag and drop the CSV file into the boxed area or click **Choose a file** and browse to the CSV file on your system. The maximum size of the CSV file is 1.2 MB.

Note Cisco DNA Center performs a validation check. An error message appears if the uploaded CSV file does not meet the following requirements:

  • The MAC address is not a valid rogue point MAC address.

  • All the rogue access point MAC addresses exist in the system already, or no rogue access point MAC addresses are eligible for the delete operation.

A green check mark indicates that the uploaded CSV file content is valid.

Step 6 Click **Next**.

Step 7 In the **Summary** window, the **Uploaded bulk allowed list MAC addresses** table displays the list of allowed MAC addresses in bulk, and the respective operation and action.

  • **All**: Shows the list of all the MAC addresses in bulk, and their respective operation and action.

  • **Create**: Shows the list of created MAC addresses in bulk, and their respective operation and action.

  • **Delete**: Shows the list of deleted MAC addresses in bulk, and their respective operation and action.

  • **No Action**: Shows the list of MAC addresses that are already deleted, and their respective operation and action.

Step 8 Click **Continue to allowed list**, and in the warning pop-up window, click **Yes**.

The **Done! Allowed List Updated** window appears.

Step 9 Click the **Go to Rogue and aWIPS Home Page** link.

The **Rogue and aWIPS** dashboard appears.

In the **Threat** table, Cisco DNA Center now categorizes the specified rogue AP MAC addresses as **Allowed List** under the **Type** column.

Step 10   To add or delete a rogue AP MAC address individually, click the rogue MAC address listed under the **Threat MAC address** column.

The **Threat 360** window appears.

Step 11   Click the **Action** drop-down list and choose **Add to Allowed list**.

To remove the rogue AP MAC address from the allowed list individually, in the **Action** drop-down list, choose **Remove from Allowed list**.

About Custom Rogue Rule Creation

Rogue rules are an easy way to segregate and manage rogues with different risk profiles. Rogue rules are easy to configure and they are applied in order of priority. They reduce false positives, noise for sites with interferers, number of alerts, and provide the ability to adjust organizational risk profiles on global and site basis.

You can move the following rogue AP types to the custom classification type:

- Interferer
- Neighbor

Create a Custom Rogue Rule

You can create a rule with specific conditions and then associate the rule to a rule profile.

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

Step 2   In the **Create a Rogue Rule** screen, click **Get Started**.

Step 3   In the **Rule Name** field, enter a unique name for the rule.

While creating new rogue rules, you cannot enter those rogue rule names that were deleted before.

Step 4   In the **Description** field, enter a description for the rule.

Step 5   Click **Next**.

Step 6   In the **Create Rogue Rule** screen, choose the threat level and add conditions for your rule.

Step 7   Select one of the **Threat Level** radio buttons to add a threat level to the rule. The available threat levels are: **High**, **Potential**, or **Informational**.

Step 8   From the **Match** drop-down list, you can either choose **All** to match all the conditions or **Any** to match any of the conditions.

Step 9   From the **Add Condition** drop-down list, choose the rule conditions.

You can add multiple conditions to a rule. The various rule conditions available are: **SSID**, **RSSI**, **Encryption Condition**, and **Minimum Rogue Client Count**.

Step 10   Click **Next**.

Step 11   To assign this rule to an existing rule profile, click **Yes** in the **Do you want to assign this rule to a rule profile?** screen.

Creating only rogue rules will not work as an entity. Rogue rules should always be assigned to a rule profile.

Step 12   In the **Available rule profiles** table, check the check box next to the profile name, and click **Next**.

You can select one or more rule profiles. You cannot assign more than five rules to a rule profile.

Step 13   In the confirmation dialog box that appears, click **Proceed**.

The created new rule is set to the lowest priority. You can edit the rule profile to change the priority.

Note   Once the rogue rule is created, you cannot use the same rogue rule name to create another rogue rule.

Step 14   Review the rogue rule configuration in the **Summary** page.

Note   Previous classification based on old rules is not modified even if the new rule conditions match. The change affects only the new data classification.

Step 15   To create another rogue rule, click the **Create Another Rogue Rule** button and follow Step 3 through Step 13 in this procedure.

Step 16   To view the created rogue rules, click the **View all Rogue Rules and Profiles** button.

The **Rogue Rules** tab lists all the rogue rules created.

You can also view the created rogue rules by navigating to this path: In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rules**.

Edit a Rogue Rule

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

Step 2   In the **Rogue Rules** table, click the rule name that you want to edit.

Step 3   In the **Edit Rogue Rule** window that appears, make the necessary changes and click **Save**.

The previous classification based on old rules is not modified even if the rule condions are modified. The change affects only the new data classification.

Delete a Rogue Rule

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

By default, the **Rogue Rules** tab is opened.

Step 2   In the **Rogue Rules** table, click the Rule Name that you want to delete and click **Delete**.

Note   If the rogue rule which you are deleting is the only rule available in a rule profile, then the rule profile is also deleted.

Step 3   Click **Delete** in the confirmation dialog box that appears.

Step 4   To view the deleted rules, click the **Inactive** tab in the **Rogue Rules** table.
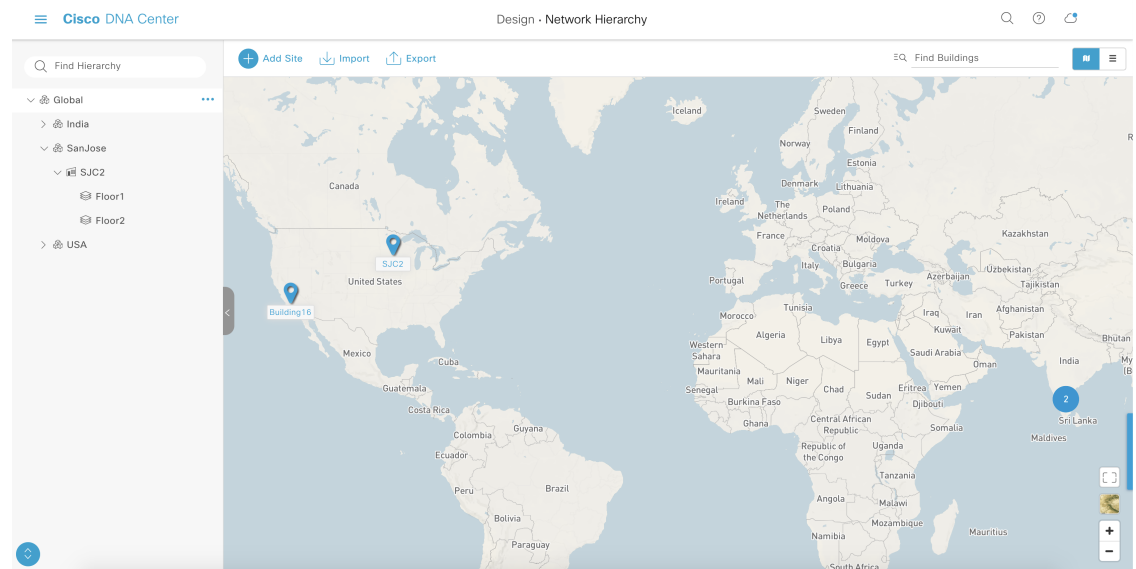
About Rogue Rule Profile

You can create a rogue rule with specific conditions and then associate it to a rule profile. You can prioritize rogue rules after associating them to a rogue rule profile.

When a rogue rule profile is assigned to a site, the rogues which are being reported from that site will be verified against the rules which are defined in the rule profile.

You can assign only one rogue rule profile to a site.

Because of the site inheritance, all floors under a particular site inherit the rogue rule profile that is mapped at the area, site, or building level. For example as shown in the below image, Floor1 and Floor2 will inherit the rogue rule profile which is mapped at the SanJose level.

A rogue rule profile mapped to a floor gets precedence over a rogue rule inherited from a parent site. For example as shown in the below image, if the Rogue Rule Profile A is directly mapped to Floor1, then the Rogue Rule Profile A takes precedence over the Rule Profile B which is assigned to the parent site which is SJC2.

Create a Rogue Rule Profile

You can create a rule with specific conditions and then associate it to a rule profile.

Step 1   In the Cisco DNA Center GUI, click the **Menu** icon (≡) and choose **Workflows** > **Create a Rogue Rule Profile**.

Step 2   In the **Create Rogue Rule Profile** screen, click **Get Started**.

Step 3   In the **Profile Name** field, enter a unique name for the rule profile.

Step 4   Click **Next**.

Step 5   In the **Rule List** table, check the check box next to the rule name, and click **Next**.

You can add up to five rogue rules in a profile.

Step 6   In the **Sort rules in order of priority** screen, drag and drop a rule into the desired priority with the highest priority on top to reorder rules based on your priority.

Step 7   Click **Next** to associate a rogue rule profile to a desired location.

Step 8   Check the check box next to the site to associate this rule profile, and click **Next**.

Rule profile can exist without being assigned to any site. Rules are not checked unless the rule profile is assigned to a site.

> **Note**   If a vendor rule and rule profile are mapped to a same site, then the vendor rule takes precedence.

Step 9   Review the rogue rule profile configuration in the **Summary** screen.

Step 10   In the **Summary** screen, click the **Back** button to make any changes to the values entered in the previous screens.

Step 11   Click **Create Rule Profile**.

A message appears, stating that the rule profile is created successfully.

Step 12   To view all rogues and profiles, click the **View all Rogue Rules and Profiles** button.

The **Rogue Rule Profiles** tab lists all the rogue rules and rule profiles created.

You can also view the created rule profiles by navigating to this path: In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Rules** > **Rogue Rule Profiles**.

Edit a Rogue Rule Profile

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

Step 2   Click the **Rogue Rule Profiles** tab.

Step 3   In the **Rogue Rule Profiles** table, click the profile name that you want to edit.

Step 4   In the **Edit Rule Profile** window that appears, make the necessary changes and click **Save**.

Edited rule profiles will not modify any previously classified data. It is applied only on the new data which is processed after changes are made.

Delete a Rogue Rule Profile

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

Step 2   Click the **Rogue Rule Profiles** tab.

Step 3   In the **Rogue Rules** table, click the profile name that you want to delete and click **Delete**.

Step 4   Click **Delete** in the confirmation dialog box that appears.

About Allowed Vendor List

With the allowed vendor list feature, you can define whether APs from specific vendors will trigger a specific threat level. You can create a list of allowed vendors, so that threats from these vendors are not marked as High Threats. You can decide whether they need to be marked as Potential or Informational threats. In a given workflow, you can add upto five vendors to the allowed list.

Allowed vendor rule which is mapped at any level takes precedence over the inherited rule. For example, if the allowed vendor rule A is mapped to a floor level, then the vendor rule A takes precedence over the allowed vendor rule B which is present at the site, area, or building level.

Create a List of Allowed Vendors

Use this procedure to create a list of vendors to be on the allowed list, so that threats from these vendors are not marked as high threats.

You can add five vendors in a single workflow for a set of sites.

Step 1   In the Cisco DNA Center GUI, click the **Menu** icon (☰) and choose **Workflows** > **Create Allowed Vendor List**.

You can also create a list of allowed vendors by clicking the **Menu** icon and choose **Assurance** > **Rogue and aWIPS** > **Allowed List** tab.

Step 2   In the **Create Allowed Vendor List** screen, click **Let's Do it**.

To skip this screen in the future, check the **Don't show this to me again** check box.

The **Create Allowed Vendor List** screen appears.

Step 3   Select a threat level to apply when the Vendor name with threat matches with the Vendor rule name from the **Threat Level** radio button.

The available threat levels are: **Potential** or **Informational**.

Step 4   From the **Selection Criteria** drop-down list, choose a selection criteria for the vendor name. The available selection criterias are: **Exactly Matches** or **Contains**.

Step 5   In the **Vendor Name** field, enter the vendor name.

The Vendor Name match is case-sensitive.

Step 6   Click ⊕ to add more vendor to the allowed.

In a given workflow, you can add a maximum of five vendors to allowed list.

Step 7   In the **Site Selection** screen, check the check box next to the site where you want to apply your allowed vendor list.

Because of the site inheritance, all floors under a particular site inherit the vendor rule that is mapped at the area, site, or building level.

Step 8   Click **Next**.

Step 9   In the **Summary** page, you can view details about the allowed vendor and site selection details.

Step 10   Click **Done**.

The **Allowed Vendor List Created** window appears.

Step 11   To create another allowed vendor list, click the **Create New Allowed Vendor List**button and follow Step 3 through Step 8 in this procedure.

Step 12   To view the created vendor list, click **View all allowed Lists**.

View Vendor Rule List Information

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

Step 2   The **Allowed Vendor List** table shows the list of allowed vendors with the following details. Each vendor rule is displayed as an entity.

- Vendor Name

- Match Criteria

- Threat Level

- Associated Site(s)

- Last Changed

Edit a Vendor Rule

This procedure shows how to edit a vendor list.

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

Step 2   In the **Allowed Vendor List** table, click the Vendor Name that you want to edit.

Step 3   In the **Edit Allowed Vendor List** window that appears which allows you to edit the following parameters:

- Threat Level

- Match Criteria

- Vendor Name

- Associated Sites

Step 4   After making the necessary changes, click **Save**.

Delete a Vendor Rule

This procedure shows how to delete a vendor.

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

Step 2 In the **Allowed Vendor List** table, check the check box of the **Vendor Name** which you want to delete, and click **Delete**.

A message saying `Deleting the selected allowed vendor(s) will impact all sites associated with it.There is 1 site associated with this allowed vendor(s)` is displayed.

Step 3 Click **Delete**.

A message saying `Selected Allowed vendor(s) deleted successfully` is displayed.

Rogue and aWIPS Event Notifications

- Rogue and aWIPS Event Notifications, on page 45

Rogue and aWIPS Event Notifications

You can configure Cisco DNA Center to send a notification whenever a rogue or aWIPS attack takes place. These events will not be logged in Cisco DNA Center Notification Center. If an event occurs after you have subscribed to "Rogue Threats" or "aWIPS threats", you can receive notifications by REST APIs (Webhook, PagerDuty, and Webex) or syslog server.

- See the "Work with Events" topic in Cisco DNA Center Platform User Guide to configure the Webhook and syslog destinations.

- See the "Cisco DNA Center to PagerDuty Integration" topic in Cisco DNA Center ITSM Integration Guide to configure the PagerDuty destination.

- See the "Cisco DNA Center to Cisco WebEx Integration" topic in Cisco DNA Center ITSM Integration Guide to configure the Webex destination.

When completing this procedure, ensure that you select and subscribe to a rogue or aWIPS event.

To subscribe to a rogue or aWIPS event in the Cisco DNA Center GUI, click the Menu icon (≡) and choose **Platform** > **Developer Toolkit** > **Events**.

Note You will receive event notifications only after subscription. For threats that occurred before subscription, in the Cisco DNA Center GUI, click the Menu icon (≡) and choose **Reports** > **Report Templates** > **Rogue and aWIPS**.

Webex and PagerDuty destinations have limits of 100 event notifications per 5 minutes. If you will receive more than 100 events in 5 minutes, configure Webhook or syslog destination.

Rogue Events

Rogue events are triggered only for the following "High" threat level rogues:

- Beacon DS Attack

- AP Impersonation

- Rogue on Wire

- Honeypot

- Custom Rules created with Threat Level as High

Rogue events are triggered when:

- High threat level rogue is discovered in network for the first time (ROGUE_NEW_THREAT_DETECTED)

- High threat level rogue is deleted in network (ROGUE_THREAT_DELETED)

- Threat level is changed from High to Potential or Informational (ROGUE_THREAT_LEVEL_CHANGED)

- Threat level is changed from Potential or Informational to High (ROGUE_THREAT_LEVEL_CHANGED)

- Threat level remains High but threat type changes (ROGUE_THREAT_TYPE_CHANGED)

Rogue Events Payload Details:

```
{
 "detectingApLocation": "string",
 "rssi": "int",
 "threatMacAddress": "string",
 "threatType": "string",
 "detectingApMacAddress": "string",
 "threatState": "string",
 "wlcIp": "string",
 "detectingApName": "string",
 "containmentState": "string",
 "vendorName": "string",
 "ssid": "string",
 "threatLevel": "string"
}
```

Commands in Payload:

- threatMacAddress - Mac Address of the Rogue Ap

- threatType - Type of Rogue threat (Beacon DS Attack, AP Impersonation, Rogue on Wire, Honeypot, or Custom Rules created with Threat Level as High)

- threatState - State of the Rogue threat (ROGUE_NEW_THREAT_DETECTED, ROGUE_THREAT_DELETED, ROGUE_THREAT_LEVEL_CHANGED), ROGUE_THREAT_LEVEL_CHANGED, or ROGUE_THREAT_TYPE_CHANGED

- threatLevel - State of the rogue (High, Potential, or Informational)

- detectingApName - Name of the strongest detecting AP

- detectingApMacAddress - MAC Address of the strongest detecting AP

- detectingApLocation - Location of strongest detecting AP

- rssi - RSSI value of the detecting AP that detects the Rogue AP

- containmentState - Containment state of the Rogue AP (PENDING, NOTCONTAINED, or CONTAINED)

- threatVendorName - Vendor Name of the Rogue AP

• ssid - Latest SSID or Honeypot SSID

• wlcIp - IP Address of the Wireless Controller

aWIPS Events

aWIPS events are triggered for all aWIPS threats in network.

Notification is sent for each Detecting AP. If multiple APs detect the same threat, you will receive multiple event notifications.

For source based aWIPS threats, source information will be sent. Destination information will be sent as "Not Applicable".

For destination based aWIPS threats, destination information will be sent. Source information will be sent as "Not Applicable".

For pair based aWIPS threats, both source and destination information will be sent.

aWIPS Events Payload Details:

```
{
 "sourceVendorName": "string",
 "detectingApLocation": "string",
 "attackType": "string",
 "sourceMacAddress": "string",
 "detectingApMacAddress": "string",
 "wlcIp": "string",
 "detectingApName": "string",
 "targetMacAddress": "string"
}
```

Commands in Payload:

• attackType - Type of the aWIPS attack

• sourceMacAddress - MAC Address of the attacker

• sourceVendorName - Vendor name of the attacker

• targetMacAddress - MAC Address of the target

• detectingApLocation - Location of the detecting AP detecting

• detectingApMacAddress - MAC Address of the detecting AP

• detectingApName - Name of the detecting AP

• wlcIp - IP Address of the Wireless Controller