Rogue AP Containment on Wired and Wireless Networks

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 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 5.

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 Click the menu icon (☰) and choose **Assurance** > **Rogue and aWIPS** > **Threats**.

Step 2 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 3 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 4 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 5 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 1: 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 6 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 7 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 2: 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 Wrong Channel	Open	Disabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled
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
Custom Rule (High, Potential)	Open	Enabled	Disabled
	Contained/Pending/Partial	Disabled	Enabled
Custom Rule (Informational)	Open	Disabled	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 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.